UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE CIENCIAS Y SISTEMAS

MAESTRÍA EN GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

CICLO ACADÉMICO 2013- 2015

Informe Final de Tesis para optar al Título de

Máster en Gestión de la Seguridad de la Información

"IMPLEMENTACIÓN DE UN SISTEMA DE PROTECCIÓN DE LA INFORMACIÓN CONFIDENCIAL EN DISPOSITIVOS PORTÁTILES DE UNIVERSIDAD CENTRAL DE NICARAGUA, EMPLEANDO TÉCNICAS DE CIFRADO CON GESTIÓN CENTRALIZADA."

Autor: Ing. Rigoberto Martín Vanegas López

Tutor: Msc. Reynaldo Castaño

Managua, Nicaragua. Noviembre, 2018

Dedicatoria

Primeramente, quiero dar gracias a Dios todopoderoso, por darme salud, trabajo, sabiduría, inteligencia, por permitirme seguir adelante en mis estudios y poco a poco ir alcanzando mis metas.

Quiero dar gracias también a mis padres, por todo su esfuerzo, consejos y su amor incondicional, por estar siempre impulsándome en mis proyectos y metas.

Gracias a Karina por su cariño, confianza, apoyo y consejos, por estar en mi vida y confiar en mí.

Gracias a mis hermanos, por estar siempre conmigo, darme fuerzas de aliento, apoyarme en todas mis decisiones y por todos sus consejos.

Gracias a mi tutor, por su apoyo, consejos y ayuda en el desarrollo de mi tesis.

Resumen del tema

Se revisó la situación actual sobre la protección de la información confidencial, en los dispositivos portátiles de la UCN, por medio de entrevistas al área de la alta dirección, se comprobó que no existe ningún método o solución implementada para proteger la información confidencial en los dispositivos portátiles, esto implica un alto riesgo de fuga de información, se probó que al retirar un disco duro sin cifrar y utilizar un enclosure, es muy fácil el acceso a la información almacenada en los discos duros, porque se encuentran legibles para cualquier persona y pueden ser utilizados para cualquier fin.

Se estudiaron diferentes características y bondades de soluciones disponibles en el mercado, basado en el cuadrante mágico de Gartner, para proponer y recomendar la mejor solución para la UCN, tomando en cuenta el precio y características. Durante el transcurso del estudio de las soluciones, se seleccionó la solución McAfee Drive Encryption, esta posee una gestión centralizada, se preparó un entorno virtual con un servidor para la consola de cifrado, un servidor de directorio activo y 6 equipos clientes para hacer las pruebas del funcionamiento de la solución.

Se comprobó que la instalación de los productos de cifrado es transparente para el usuario final, una vez que el disco duro está cifrado, únicamente se puede acceder con usuarios autorizados, en caso de daño en algún hardware que no sea el disco duro del dispositivo portátil, esta información no se pierde, existen métodos propios de la solución para la recuperación de la misma. Se verificó que el proceso de recuperación de equipo en caso que no se pueda ingresar por olvido de contraseña o bloqueo de usuario por varios intentos fallidos es muy sencillo siempre y cuando se tenga acceso a la consola de cifrado. Una vez cifrado el disco se volvió a realizar la prueba de retirarlo y usar un enclosure, no se pudo acceder a la información porque se encontraba protegido por la solución de cifrado.

1. Tabla de contenido

1. Introducción

Actualmente en Nicaragua, la seguridad de la información es un tema novedoso y no muchas empresas invierten en proyectos que les garanticen que únicamente las personas autorizadas puedan tener acceso a la información.

En la UCN, no existe ninguna solución para proteger la información contenida en sus discos duros de los dispositivos portátiles, este tema es preocupante porque esta información valiosa puede caer en personal no autorizado en caso de pérdida o robo de los dispositivos.

Al implementar una solución de cifrado en los dispositivos portátiles en la UCN, la administración es centralizada y el cifrado se realiza de manera transparente para los usuarios finales desde la consola. En el caso de que un dispositivo portátil se extravíe producto de un robo o confusión, esta información confidencial será ilegible y no será obtenida por ningún método de recuperación que no sea el recomendado por la solución, de tal manera que los propietarios de la información estarán protegidos, porque la información no caerá en manos equivocadas y se evitará la fuga de información.

La presente investigación tiene la finalidad de revisar cuatro opciones del mercado basado en el cuadrante mágico de Gartner y seleccionar la más optima según las necesidades de la UCN e implementar el sistema de protección de la información confidencial en dispositivos portátiles, empleando técnicas de cifrado con gestión centralizada.

2. Definición de los Objetivos

2.1. Objetivo General

- Diseñar un sistema de protección de la información confidencial en dispositivos portátiles de la Universidad Central de Nicaragua, empleando técnicas de cifrado con gestión centralizada.

2.2. Objetivos Específicos

- Analizar la situación actual de los mecanismos de protección de la información implementados en la Universidad Central de Nicaragua.

- Evaluar soluciones de seguridad que faciliten la protección de la información de los dispositivos portátiles.

- Diseñar la infraestructura de seguridad necesaria para la implementación del sistema de protección.

3. Justificación

En los dispositivos portátiles que no se protege la información contenida en su disco duro, por medio de una solución de cifrado, está expuesta a que esta información sea fácil de acceder, porque se encuentra legible para todos. En la UCN se han presentados varios casos de pérdida o robo de dispositivos portátiles, estos incidentes han afectado negativamente porque la información fue fácilmente accedida porque no se encontraba protegida.

Para garantizar en la UCN la confidencialidad, autenticidad o integridad de la información, se implementará un sistema de protección de la información confidencial en dispositivos portátiles, empleando técnicas de cifrado con gestión centralizada.

Este proyecto de solución de cifrado se integrará con un sistema de autenticación única (Single Sign-On), a través de un servidor de directorio activo existente, esto con el objetivo de que las contraseñas no sean administradas de maneras locales, si no que estas se encuentren guardadas en el directorio activo, se programará una tarea automática para la sincronización de los usuarios con el directorio activo, con el objetivo de garantizar que la clave válida sea la del servidor de directorio activo.

Al implementar esta solución en la UCN, se mitiga la fuga de información y se garantiza que la información solo sea accedida por personal autorizado, esta información contenida en su disco duro no podrá ser utilizada para otros fines, porque se encuentra ilegible para personal no autorizado.
Es de gran importancia que esta solución se implemente en la UCN, para proteger los 100 dispositivos portátiles (laptops) que se encuentra actualmente en su inventario.

4. Antecedentes

En años anteriores en la UCN se han presentado varios incidentes de pérdidas de dispositivos portátiles, la información contenida en estos dispositivos no se encontraba protegida por ninguna solución, no se pudo evitar que esta información fuera obtenida por personal no autorizado.

Una cuenta de usuario protegida con contraseña no protege tu información (Stewart, 2018). Aunque la contraseña evitará que alguien más acceda a tu computadora, los atacantes pueden utilizar otros métodos para copiar los archivos.

Si los ladrones quitan el disco duro y lo ponen en otra computadora, tendrán acceso a cualquier archivo que hayas almacenado ahí. En algunos casos, incluso pueden restaurar la contraseña de tu computadora y obtener acceso a tu correo electrónico, tus otras contraseñas y más datos personales.

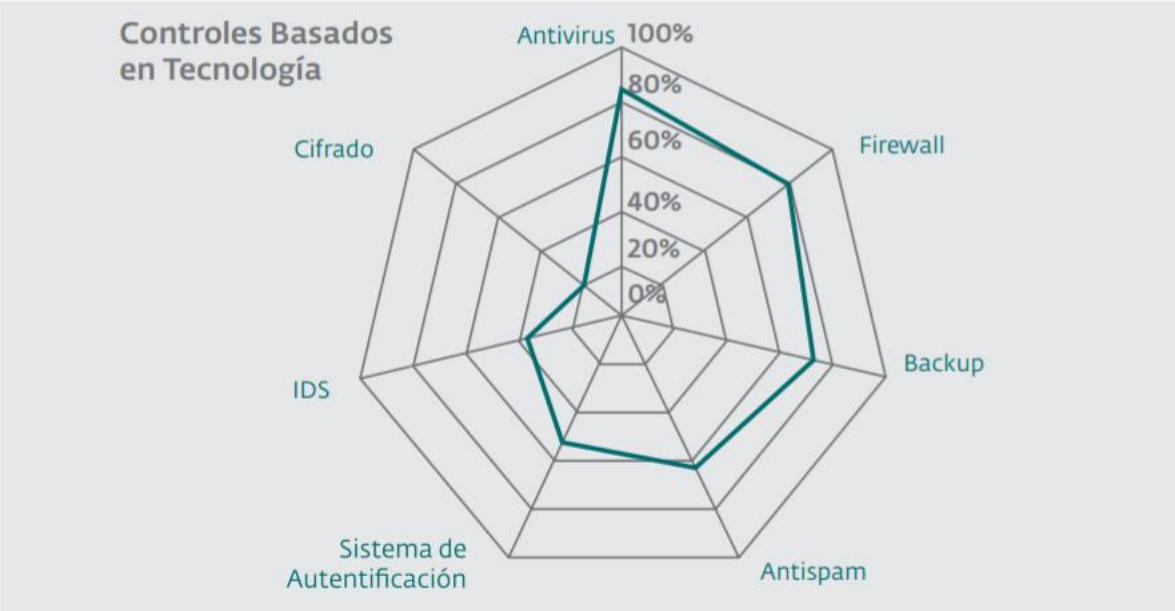
Por fortuna, puedes proteger tu información de estos tipos de ataques con una encriptación. (Gordon, 2018).

Por medio de una encuesta realizada por Eset Latinoamérica, el 58,6% de los usuarios afirmó que le han robado su teléfono móvil. Le siguen las personas a las que nunca les han robado el dispositivo (36,7%), las computadoras portátiles (*notebook*) con un 6,1% y las *netbooks* con 3%. Las tabletas quedan relegadas al último lugar con el 1,6% de las elecciones. (Eset, 2013).

Solo el 20% de las empresas de Latinoamérica utilizan cifrado para proteger su información, de acuerdo con el ESET Security Report 2013.

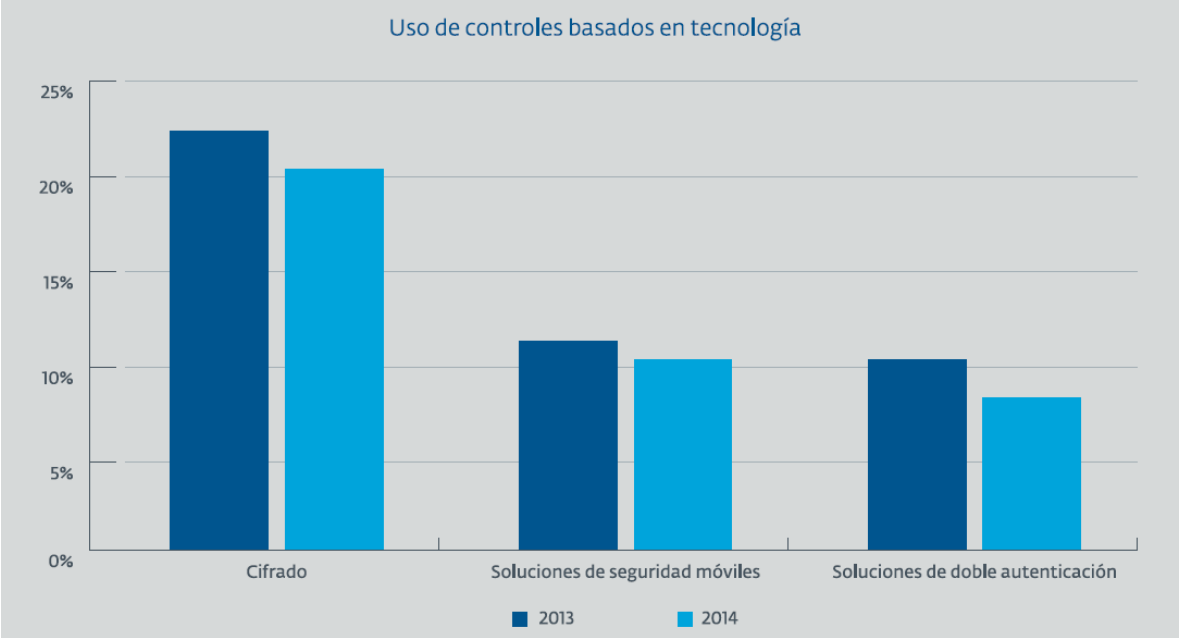
Figura 1. Controles Basados en Tecnología.

Fuente ESET Security Report | Latinoamérica 2013



Fuente: (Eset:2013. 5)

Figura 2. Uso de controles tecnológicos durante 2013 y 2014.



Fuente: (Eset:2015. 17)

5. Marco Teórico

La información es un activo valioso que puede impulsar o destruir su empresa. Si se gestiona de forma adecuada, le permite trabajar con confianza. La gestión de la Seguridad de la Información le ofrece la libertad para crecer, innovar y ampliar su base de clientes sabiendo que toda su información confidencial seguirá siéndolo. (Bsigroup.com, 2017).

La seguridad de la información se logra implementando un conjunto adecuado de controles, políticas, procesos, procedimientos, estructuras organizacionales, y otras acciones que hagan que la información pueda ser accedida sólo por aquellas personas que están debidamente autorizadas para hacerlo. (jaimemontoya, 2017).

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos. (Iso27001, 2017).

La seguridad de la información, según la ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Figura 3. Pilares de seguridad de la información.

Fuente: (ISO 27001)

- **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran. (Iso27001, 2017).

5.1. Criptografía

La palabra criptografía viene del griego cripto (que significa «ocultar») y graphos (que significa «escribir»). Se podría traducir por: **cómo escribir mensajes ocultos**. En la antigüedad se utilizaba sobre todo durante las guerras, para comunicar estrategias, de manera que, aunque el mensajero fuera interceptado por el enemigo, el contenido del mensaje estaba a salvo. (Roa Buendía, 2013:29).

La criptografía consiste en tomar el documento original y aplicarle un **algoritmo** cuyo resultado es un nuevo documento. Ese documento está cifrado: no se puede entender nada al leerlo directamente. Podemos, tranquilamente,

hacerlo llegar hasta el destinatario, que sabrá aplicar el algoritmo para recuperar el documento original. (Roa Buendía, 2013:29).

Las claves son combinaciones de símbolos (letras, números, signos de puntuación, etc.). Por tanto, nuestra seguridad está expuesta a los **ataques de fuerza bruta:** probar todas las combinaciones posibles de símbolos. Para evitarlo tomaremos estas medidas:

- **Utilizar claves de gran longitud (512-1024-2048-4096 bytes)**, de manera que el atacante necesite muchos recursos computacionales para cubrir todo el rango rápidamente.
- **Cambiar regularmente la clave.** De esta forma, si alguien quiere intentar cubrir todo el rango de claves, le limitamos el tiempo para hacerlo.
- **Utilizar todos los tipos de caracteres posibles:** una clave compuesta solo de números (diez valores posibles) es más fácil de adivinar que una con números y letras (36 valores posibles).
- **No utilizar palabras fácilmente identificables:** palabras de diccionario, nombres propios, etc.
- **Detectar repetidos intentos fallidos en un corto intervalo de tiempo.** Por ejemplo, la tarjeta del móvil se bloquea si fallamos tres veces al introducir el PIN.

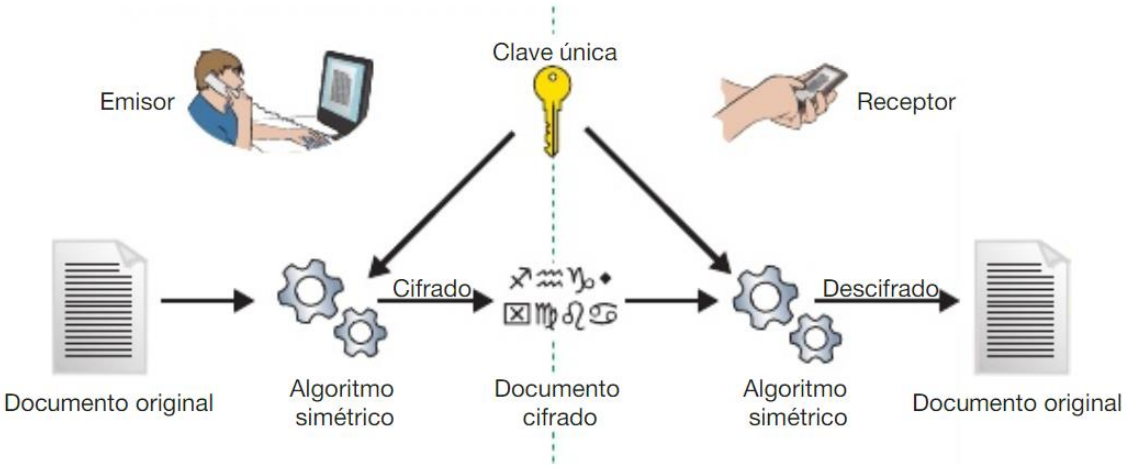
Las claves no son el único punto débil de la criptografía; pueden existir vulnerabilidades en el propio algoritmo o en la implementación del algoritmo en alguna versión de un sistema operativo o un driver concreto. Estas vulnerabilidades las estudia el criptoanálisis. (Roa Buendía, 2013:29).

5.1.1. Criptografía simétrica y asimétrica

Los algoritmos de criptografía simétrica utilizan la misma clave para los dos procesos: cifrar y descifrar. Son sencillos de utilizar y, en general, resultan bastante eficientes (tardan poco tiempo en cifrar o descifrar). Por este motivo, todos los algoritmos, desde la antigüedad hasta los años setenta, eran simétricos. Los más utilizados actualmente son DES, 3DES, AES, Blowfish e IDEA.

El funcionamiento es simple: en la Figura 4 el emisor quiere hacer llegar un documento al receptor. Toma ese documento y le aplica el algoritmo simétrico, usando la clave única, que también conoce el receptor. El resultado es un documento cifrado que ya podemos enviar tranquilamente.
Cuando el receptor recibe este documento cifrado, le aplica el mismo algoritmo con la misma clave, pero ahora en función de descifrar. Si el documento cifrado no ha sido alterado en el camino y la clave es la misma, el resultado será el documento original.

Figura 4. Criptografía simétrica.



Fuente: (Roa:2013. 30)

El problema principal de la criptografía simétrica es la circulación de las claves: cómo conseguimos que el emisor y el receptor tengan la clave buena. No podemos utilizar el mismo canal inseguro por el que enviaremos el mensaje (la inseguridad nos ha llevado a cifrar). Hay que utilizar un segundo canal de comunicación, que también habría que proteger, y así sucesivamente. Por ejemplo, en el correo de bienvenida a una empresa puede aparecer la contraseña de la wifi de la oficina; cuando se cambie, se envía otro correo, etc. (Roa Buendía, 2013:34).

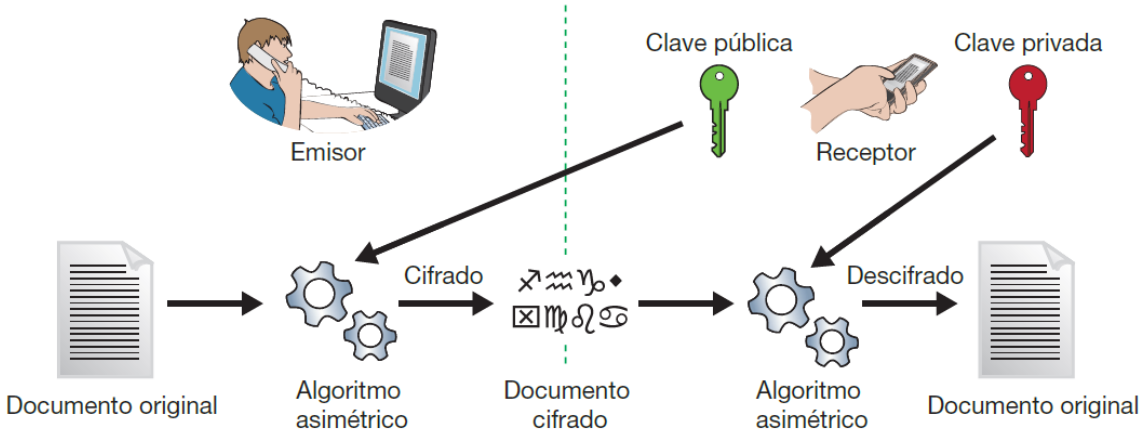
El segundo problema es la gestión de las claves almacenadas. Si en una empresa hay diez trabajadores y todos tienen conversaciones privadas con todos, cada uno necesita establecer nueve claves distintas y encontrar nueve canales seguros para actualizarlas cada vez (en total 81 claves y 81 canales). Si aparece un trabajador nuevo, ahora son 100 claves y 100 canales. Y las empresas pueden tener muchos trabajadores: 500, 5,000, 50,000... ¿Cada vez que cambie mi clave tengo que avisar a 49 999 compañeros? Es poco manejable. (Roa Buendía, 2013:34).

En los años setenta, los criptógrafos Diffie y Hellman publicaron sus investigaciones sobre criptografía asimétrica. Su algoritmo de cifrado utiliza dos claves matemáticamente relacionadas de manera que lo que cifras con una solo lo puedes descifrar con la otra. Comparado con la clave simétrica, ahora el emisor no necesita conocer y proteger una clave propia; es el receptor quien tiene el par de claves. Elige una de ellas (llamada clave pública) para comunicarla al emisor por si quiere enviarle algo cifrado. Pero ya no hace falta buscar canales protegidos para enviarla porque, aunque un tercer individuo la conozca, todo lo que se cifre con esa clave solo se podrá descifrar con la otra clave de la pareja (la clave privada), que nunca es comunicada. Y matemáticamente es imposible deducir la clave privada conociendo solo la clave pública. (Roa Buendía, 2013:34).
Como se ilustra en la figura 5, cuando el emisor quiere hacer llegar un mensaje confidencial al receptor, primero consigue la clave pública del receptor. Con esa

clave y el documento original, aplica el algoritmo asimétrico. El resultado es un documento cifrado que puede enviar al receptor por cualquier canal. Cuando el mensaje cifrado llega al receptor, él recupera el documento original aplicando el algoritmo asimétrico con su clave privada.

Si el receptor quiere enviar al emisor una respuesta cifrada, debería conseguir la clave pública del emisor y seguir el mismo procedimiento. (Roa Buendía, 2013:34).

Figura 5. Criptografía asimétrica.



Fuente: (Roa:2013. 34)

La criptografía asimétrica resuelve los dos problemas de la clave simétrica:

- No necesitamos canales seguros para comunicar la clave que utilizaremos en el cifrado.
- No hay desbordamiento en el tratamiento de claves y canales. Si somos nueve empleados, solo necesitamos nueve claves y un solo canal: la intranet de la empresa, un correo destinado a toda la empresa, etc. Y si aparece un empleado nuevo, serán diez claves y el mismo canal.

Sin embargo, los algoritmos asimétricos tienen sus propios problemas:

- Son poco eficientes: tardan bastante en aplicar las claves para generar los documentos cifrados, sobre todo porque las claves deben ser largas para asegurar la independencia matemática entre ellas.
- Utilizar las claves privadas repetidamente es arriesgado porque algunos ataques criptográficos se basan en analizar paquetes cifrados. Estos paquetes serían capturados en la red o directamente el atacante podría elaborar un software malicioso que generase paquetes de tamaño y contenido elegidos cuidadosamente y conseguir enviarlos a nuestro servidor para que los devolviera cifrados con su clave privada.
- Hay que proteger la clave privada. No basta con dejarla en un fichero de una carpeta del disco duro en la cuenta de nuestro usuario; cualquier otro usuario con permisos de administrador podría llegar hasta él. Por este motivo, las claves privadas se guardan todas juntas en un fichero llamado keyring (archivo de llaves, llavero), y este fichero está protegido mediante cifrado simétrico. Es decir, para poder usar la clave privada, hay que introducir una clave que descifra el llavero y permite leerla.

Necesitamos una segunda medida de protección de la clave privada: la copia de seguridad del llavero. Si el disco duro se estropea, perderemos el fichero que contiene la clave privada y no podremos volver a utilizarla. Por tanto, debemos incluirlo en la política de backup de la empresa, y confiamos en que, aunque alguien más tenga acceso al backup (cintas, discos, etc.), la clave simétrica todavía protege el llavero.

- Hay que transportar la clave privada. En cifrado simétrico, si hemos enviado el fichero cifrado a otra máquina y queremos descifrarlo, basta con recordar la clave e introducirla. Pero en la clave privada esto es imposible (son cientos de símbolos sin sentido). Debemos transportar el llavero, con el riesgo que supone (si lo perdemos, podrían intentar un ataque de fuerza bruta contra el cifrado simétrico).

5.1.2. Cifrado

Cifrar o encriptar datos significa alterarlos, generalmente mediante el uso de una clave, de modo que no sean legibles para quienes no posean dicha clave. Luego, a través del proceso de descifrado, aquellos que sí poseen la clave podrán utilizarla para obtener la información original. Esta técnica protege la información sensible de una organización, ya que, si los datos cifrados son interceptados, no podrán ser leídos. (Eset-la, 2014).

Una de las primeras técnicas de cifrado que se usó en la historia fue el “código del César”, que consistía en remplazar cada letra de un mensaje por otra que se encontrara más adelante en el alfabeto. Debido a su baja complejidad, se idearon otros métodos, por ejemplo, tatuar las claves de descifrado en los esclavos. (Eset-la, 2014).

5.1.3. Cifrado de Discos

El cifrado de disco es una tecnología que protege la información convirtiéndola en código ilegible que no puede ser descifrado fácilmente por personas sin autorización. El cifrado de disco utiliza un software de encriptación o un hardware de encriptación para cifrar cada bit de información que va en un disco o en volumen de disco. El cifrado de disco evita el acceso no autorizado a información almacenada.

Expresiones como cifrado de disco llena (FDE) o cifrado de disco completa generalmente significan que todo en el disco está encriptado incluyendo los programas que pueden cifrar particiones de sistemas operativos de arranque sin embargo, cuando se separa el disco no necesariamente está cifrado. En los sistemas que usan un registro de inicio maestro (MBR), parte del disco

permanece sin cifrar. Algunos sistemas de cifrado de disco completos basados en hardware pueden cifrar un disco de arranque, incluyendo el MBR. (Cifrado de Disco, 2017).

5.1.4. Cifrado Transparente

El cifrado transparente, también conocido como cifrado en tiempo real y cifrado al momento (OTFE), es un método usado por algunos programas de cifrado de discos. "Transparente" se refiere al hecho de que los datos son automáticamente cifrados o descifrados al mismo tiempo que son cargados o guardados. (Cifrado de Disco, 2017).

Con el cifrado transparente, los archivos se vuelven accesibles inmediatamente después de que se da una llave, y el volumen completo es generalmente montado si existe un controlador físico, haciendo los archivos tan accesibles como cualquier otro que esté desencriptado. Ningún dato que esté almacenado en un volumen cifrado puede ser leído (descifrado) sin usar contraseña/archivo clave o clave de cifrado. Todo el sistema de archivos que no posea un volumen está cifrado (incluyendo nombres de archivos, nombres de carpeta, contenidos y otros meta-datos). (Cifrado de Disco, 2017).

5.1.5. Protección de Información

Cifrar los datos implica que cada vez que se quiera acceder a los mismos, se deban descifrar, lo que agrega un nivel de complejidad al acceso simple, pero reduce la velocidad del proceso. A raíz de esto, surgen ciertas preguntas: ¿por qué hay que cifrar la información importante en una empresa? ¿Cuáles son los beneficios de hacerlo?

Es muy difícil para una compañía poder revertir el daño generado luego de una intrusión significativa, por lo que es fundamental tomar las medidas necesarias para evitarlas y, si ocurren, contar con la preparación adecuada para minimizar el riesgo, por ejemplo, utilizando datos cifrados.

5.1.6. Beneficios del Cifrado

- **Proteger la información confidencial de una organización.**

Si la información sensible de una compañía llegara a caer en las manos equivocadas, pueden producirse perjuicios económicos, pérdidas de ventaja competitiva, o incluso significar el cierre de la empresa. En este sentido, la encriptación ayuda a proteger Información delicada, como los datos financieros, de los colaboradores, procedimientos o políticas internas, entre otros (Eset-la, 2014).

- **Proteger la imagen y el prestigio de una organización.**

Existe cierta información que, si es robada, puede dañar la imagen corporativa. Un ejemplo notable, son los datos que se almacenan de los clientes; el robo de los mismos puede afectar considerablemente a la empresa, llevándola a pérdidas irrecuperables (Eset-la, 2014).

- **Proteger dispositivos móviles e inalámbricos.**

Todos aquellos dispositivos que salen de la empresa, como teléfonos celulares, tabletas o computadoras portátiles, pueden ser extraviados y/o robados. Ante estas situaciones, es importante asegurarse de que ningún tercero esté autorizado pueda acceder a la información (Eset-la, 2014).

5.1.7. Protección de dispositivos portátiles

La información es un activo muy importante y valioso para las organizaciones, razón por la cual hay que resguardarla de manera segura y que únicamente tengan acceso personal autorizado.

La información almacenada en estos dispositivos es necesario protegerla implementando una solución de cifrado para impedir la fuga de los datos confidenciales, en particular en caso de pérdida o robo del mismo. Antes de iniciar a implementar con una solución de cifrado es importante realizar un respaldo de toda la información contenida en el disco duro de los dispositivos portátiles.

5.1.8. Cifrado de datos locales

La información que no es transmitida también corre el riesgo de ser accedida por terceros; por ejemplo, ante el extravío o robo de los equipos portátiles.
La contraseña de inicio de sesión no es suficiente para proteger los datos, y es allí donde el cifrado entra en juego. En este sentido, puede cifrarse el disco entero, de tal manera que cada vez que se encienda la computadora se deba ingresar la clave para tener acceso a la misma. Este enfoque suele ser el elegido en las empresas, aunque también existe la alternativa de cifrar sólo algunas carpetas o archivos específicos. Además, cabe aclarar que esto se puede extender a cualquier dispositivo que transporte información delicada, como memorias USB (Eset-la, 2014).

La información de los clientes es sumamente importante y, de no poder garantizar la seguridad de la misma, los clientes dejarán de confiar en la empresa. Un ejemplo de esto se da en el almacenamiento de los datos de autenticación de los usuarios: si las contraseñas se almacenaran en una base sin cifrar, las cuentas

de los clientes se verían directamente comprometidas si un atacante lograse acceder a estos registros (Eset-la, 2014).

5.1.9. Soluciones de Cifrados

Las soluciones de cifrado cifran ordenadores de escritorio y portátiles, medios extraíbles, CD-ROM, archivos de red, dispositivos de almacenamiento en la nube, otros dispositivos y el correo electrónico para proteger los datos. Para acceder a la información, es necesario utilizar las claves adecuadas para descifrar los datos mediante una contraseña.

Estas soluciones vienen diseñadas para que los datos del disco de los sistemas sean ininteligibles para las personas no autorizadas, lo que a su vez ayuda a cumplir los requisitos de las normativas.

5.1.9.1. Algunos Beneficios

- Aplica un riguroso control de acceso con autenticación previa al arranque.
- Activa el cifrado automático y transparente sin entorpecer el rendimiento.
- Admite entornos de dispositivos mixtos, incluidas unidades de estado sólido.
- Compatible con las unidades con autocifrado TCG Opal v1.0 (solo PC).
- Protege contra el acceso no autorizado cuando las computadoras portátiles se pierden o son robadas.
- Mayor rendimiento gracias a la compatibilidad con la tecnología Intel AES-NI.
- Solución de punto final con una sola consola y administración centralizada.

5.2. Cuadrante Mágico para plataformas de Protección de Endpoint

La Plataforma de Protección de Endpoint empresarial por sus siglas en inglés (EPP) es una solución integrada que tiene las siguientes capacidades:
Anti-malware, Personal firewall, Port and device control, Vulnerability assessment, Application control and application sandboxing, Enterprise mobility management (EMM), Memory protection, Endpoint detection and response (EDR) technology, **Data protection such as full disk and file encryption**, Endpoint data loss prevention (DLP).

Figura 6. Cuadrante Mágico de Gartner.

Fuente: (Gartner, 2018)

5.3. Aplicaciones de cifrado de disco completo

En el mercado existen muchas aplicaciones disponibles que permiten el cifrado completo de discos duros. Sin embargo, varían en gran medida en características y seguridad. En esta investigación analizamos 4 aplicaciones basándonos en cuadrante mágico de Gartner.

5.3.1. McAfee Drive Encryption

También llamado encriptación total de disco, es un software de encriptación que ayuda a proteger los datos de las tablets, portátiles y PCs con Microsoft Windows instalado para impedir la fuga de datos confidenciales, en particular en caso de pérdida o robo. Está diseñado para que todos los datos del disco de los sistemas sean ininteligibles para las personas no autorizadas, lo que a su vez ayuda a cumplir los requisitos de las normativas (McAfee, 2016).

Admite discos duros tradicionales (discos giratorios o HDD), discos de estado sólido (SSD) y discos de encriptación automática (SED y OPAL). Drive Encryption es un componente de software de tres suites de protección de datos y puntos terminales de McAfee, y se gestiona mediante la consola de administración de McAfee ePolicy Orchestrator (McAfee ePO). (McAfee, 2016).

5.3.2. Principales Beneficios

- Aplica un riguroso control de acceso con autenticación previa al arranque.
- Utiliza algoritmos de encriptación certificados (FIPS, Common Criteria) utilizados por las Fuerzas Armadas. Ha recibido las certificaciones FIPS 140-2, Common Criteria EAL2+ e Intel Advanced Encryption Standard–New Instructions (AES–NI).
- Activa la encriptación automática y transparente sin entorpecer el rendimiento.
- Admite ambientes de dispositivos mixtos, incluidas unidades de estado sólido.
- Admite unidades de encriptación automática OPAL de Trusted Computing Group (TCG).

McAfee Drive Encryption ofrece un cifrado potente que protege los datos del acceso no autorizado, la pérdida y la exposición. Debido a que las brechas de datos están en aumento, es importante proteger los activos de información y cumplir con las normas de privacidad. (McAfee, 2016).

5.3.2.1. Protección Integral

La suite McAfee Drive Encryption proporciona múltiples capas de defensa contra la pérdida de datos con varios módulos integrados que abordan áreas específicas de riesgo. La suite proporciona protección para ordenadores individuales y ordenadores portátiles móviles con el BIOS (Basic Input Output System), la interfaz de firmware extensible (EFI) y la interfaz de firmware extensible unificada (UEFI, Unified Extensible Firmware Interface). (McAfee, 2015).

¿Qué es McAfee Drive Encryption?

McAfee Drive Encryption es una potente utilidad criptográfica para denegar el acceso no autorizado a los datos almacenados en cualquier sistema o disco cuando no esté en uso.
Evita la pérdida de datos sensibles, especialmente de equipos perdidos o robados. Protege los datos con control de acceso mediante la autenticación de pre-arranque y un potente motor de cifrado.
Para iniciar sesión en un sistema, el usuario debe primero autenticarse a través del entorno de pre-arranque. En la autenticación exitosa, el sistema operativo del sistema cliente se carga y da acceso al funcionamiento normal del sistema.

McAfee Drive Encryption compuesto por el software de cifrado instalado en los sistemas cliente y el componente de administración de los servidores. Se implementa y administra a través de McAfee ePolicy Orchestrator® (McAfee ePO) mediante políticas. Una política es un conjunto de reglas que determina cómo funciona el software McAfee Drive Encryption en el equipo del usuario.

El proceso de cifrado de disco es completamente transparente para el usuario y tiene poco impacto en el rendimiento de la computadora.

5.3.2.2. Cómo funciona McAfee Drive Encryption

McAfee Drive Encryption protege los datos de un sistema mediante el control del disco duro o de la unidad de cifrado automático (Opal) del sistema operativo. Cuando se utiliza con unidades de cifrado automático, Drive Encryption gestiona las claves de autenticación de disco; con unidades que no se cifran automáticamente. El controlador Drive Encryption cifra todos los datos escritos en el disco y descifra los datos leídos del disco.

El software McAfee Drive Encryption está instalado en el sistema cliente. Una vez finalizada la instalación, y dependiendo de la directiva de Encriptación de unidad asignada al sistema cliente, el sistema cliente comienza a activar el cifrado de unidad. El cifrado comienza sólo cuando se activa con éxito. Durante el proceso de activación, el sistema se sincroniza con McAfee ePO y adquiere datos de usuario, datos de token y datos de tema de Pre-Boot. La autenticación previa a la inicialización no aparece si el sistema se reinicia durante el proceso de activación.

Drive Encryption toma el control del disco sólo después de que el proceso de activación se haya completado correctamente. A continuación, comienza a aplicar la política de cifrado. Después de la activación y el reinicio del sistema, el usuario se autentica e inicia sesión a través del entorno de pre-inicio, que luego carga el sistema operativo.

5.3.2.3. Servidor ePO de McAfee

El servidor McAfee ePO proporciona una plataforma escalable para la administración centralizada de políticas y el cumplimiento de sus productos y sistemas de seguridad donde residen. La consola ePO de McAfee:

- Le permite administrar las directivas de McAfee Drive Encryption en el equipo cliente.
- Le permite implementar y administrar productos McAfee Drive Encryption.
- Proporciona capacidades integrales de generación de informes y despliegue de productos; todo a través de un único punto de control.

5.3.2.3.1. Políticas

McAfee Drive Encryption se administra a través de McAfee ePO mediante una combinación de directivas basadas en el usuario y políticas de configuración del producto. La consola ePO de McAfee le permite aplicar directivas a través de grupos de equipos o en una sola computadora. Cualquier nueva aplicación de políticas a través de McAfee ePO anula la directiva existente que ya está establecida en los sistemas individuales. (McAfee, 2015).

5.3.2.3.2. Extensiones y paquetes de productos

La extensión Drive Encryption instalada en McAfee ePO define el algoritmo de cifrado, la configuración del producto y la configuración del servidor para el sistema cliente. Los paquetes de software de Drive Encryption registrados en McAfee ePO definen el software de Drive Encryption que está instalado en el sistema cliente. (McAfee, 2015).

5.3.2.3.3. Administrador de cifrado de unidad

El sistema de administración de Drive Encryption, Drive Encryption Admin, define las configuraciones genéricas de Drive Encryption para las políticas de configuración del producto, las políticas basadas en el usuario, las configuraciones de usuario del dominio local y la configuración del servidor de usuario. (McAfee, 2015).

5.3.2.4. Servidor LDAP

Drive Encryption adquiere usuarios a través de Windows Active Directory (AD) o a través del directorio de usuarios de McAfee ePO. Debe tener un servidor LDAP registrado o tener instalado el Directorio de usuarios para poder utilizar reglas de asignación de políticas para habilitar conjuntos de permisos asignados dinámicamente y para habilitar la creación manual y automática de cuentas de usuario. (McAfee, 2015).

5.3.2.5. Características

Estas características de Drive Encryption son importantes para la seguridad y protección del sistema de su organización.

- **Gestión centralizada:** Drive Encryption se integra completamente en McAfee ePO, aprovechando la infraestructura ePO de McAfee para la generación de informes, la supervisión, la implementación y la administración de políticas automatizadas de seguridad.

- **Cifrado transparente:** Drive Encryption permite el cifrado transparente sin obstaculizar el rendimiento de los usuarios o del sistema.

- **Control de acceso:** Drive Encryption impone un control de acceso sólido con la autenticación de pre-arranque.

- **Capacidad de administración remota:** Drive Encryption es compatible con la tecnología de administración activa Intel® (Intel® AMT) para administrar y proteger remotamente los sistemas junto con McAfee® ePO Deep Command.

- **Recuperación:** La función de recuperación permite al usuario final realizar una recuperación de emergencia cuando el sistema no se reinicia o su sistema de archivos de prearranque (PBFS) está dañado.

- **Compatibilidad con unidades de cifrado automático:** La combinación de Drive Encryption y McAfee ePO permite la administración centralizada de unidades de autoencriptación que se ajustan al estándar Opal de Trusted Computing Group (TCG), incluyendo el bloqueo y desbloqueo, la generación de informes, la recuperación, y la gestión de usuarios. Para obtener más información, consulte Opal auto-cifrado unidades.

- **Módulo de plataforma de confianza (TPM):** Drive Encryption admite TPM 2.0 en los sistemas UEFI de Windows 8 para proporcionar autenticación de plataforma sin necesidad de autenticación previa a la inicialización (PBA).

- **Actualización del sistema operativo:** Los usuarios pueden realizar una actualización / actualización principal del sistema operativo Windows del sistema que esté cifrada con Drive Encryption 7.1 o versiones anteriores. Este proceso conservará el estado de cifrado para todo el proceso. (McAfee, 2015).

5.3.2.6. Requerimientos para la instalación de MDE

Asegúrese de que su servidor y su sistema cliente cumplan con estos requisitos previos antes de instalar Drive Encryption.

Tabla 1. Requerimiento de Sistemas.

Systems	Requirements
McAfee ePO server systems	See the product documentation for your version of McAfee ePO.
Client systems	• **CPU**: Pentium III 1 GHz or higher • **RAM**: 512 MB minimum (1 GB recommended) • **Hard Disk**: 200 MB minimum free disk space

Fuente: (McAfee:2018. 5)

Tabla 2. Requerimiento de Software.

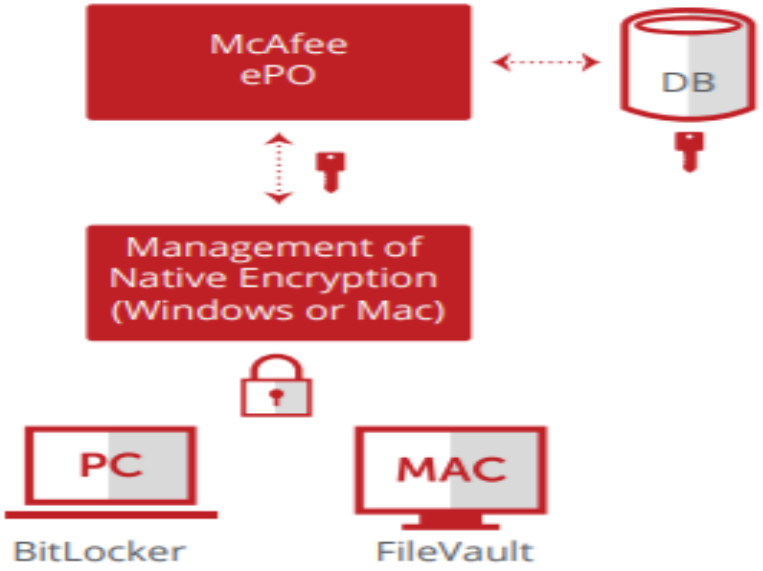
Systems	Requirements
McAfee ePO	5.3.x or higher
Drive Encryption	Extensions: • `EEAdmin.zip` • `EEPC.zip` • `help_de_720.zip` • `EEGO.zip` • `UserDirectory.zip`
	Software packages: • `MfeEEPC.zip` • `MfeEEAgent.zip`
Microsoft Windows Installer 3.0 Redistributable package (for McAfee ePO)	See the product documentation for your version of McAfee ePO.
Microsoft .NET Framework 2.0 Redistributable package (for McAfee ePO)	See the product documentation for your version of McAfee ePO.
Microsoft MSXML 6 (for McAfee ePO)	See the product documentation for your version of McAfee ePO.

Fuente: (McAfee:2018. 5)

5.3.2.7. Gestión del cifrado nativo para Windows y Macs

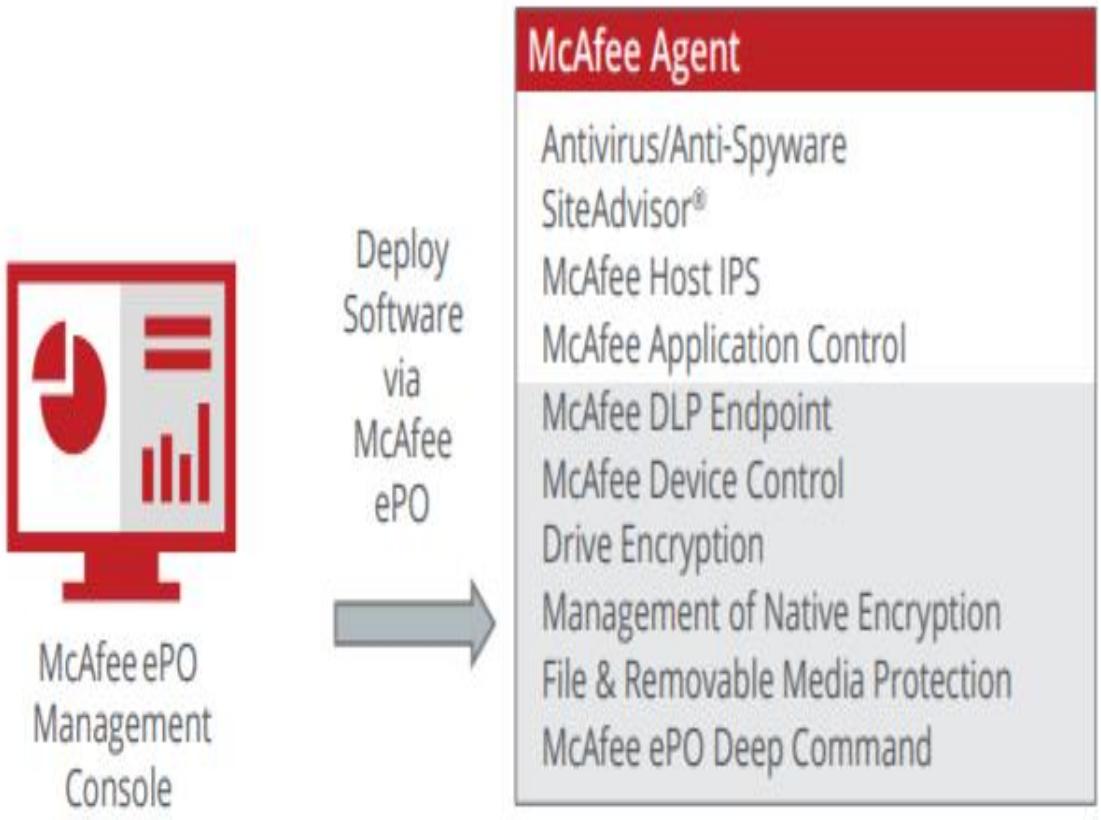
Apple y Microsoft ofrecen un software integrado de cifrado, diseñado para que los datos de las unidades de los sistemas sean ininteligibles para las personas no autorizadas. Apple FileVault es una función estándar de Mac OS X y Microsoft BitLocker es parte de las versiones de Windows para empresas. Management of Native Encryption de McAfee, componente de software disponible en varias suites de protección de datos y endpoints, permite administrar a través de la consola de McAfee ePolicy Orchestrator (McAfee ePO) cualquier combinación de endpoints que tengan FileVault y BitLocker habilitados.

Imagen 7. Administración del cifrado nativo para Windows y Macs.



Fuente: (McAfee:2016. 3)

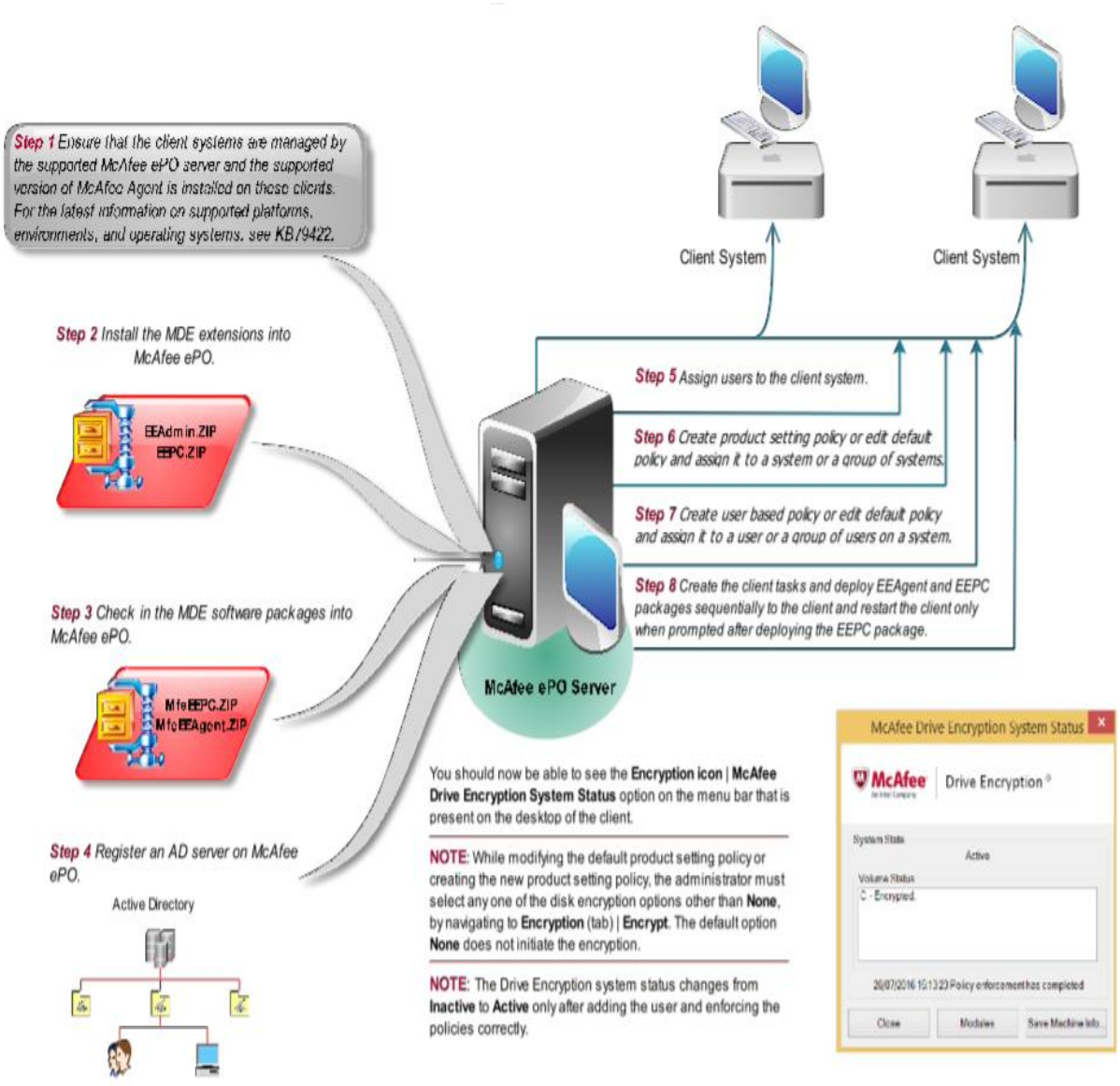
Imagen 8. Productos desplegados de consola ePO.



Fuente: (McAfee:2016. 3)

En la imagen 9, se muestra un inicio rápido y especifica la lista de verificación de requisitos previos para ayudarlo rápidamente a comprender el proceso de instalación de McAfee Drive Encryption.

Imagen 9. Instalación MDE.



Fuente: (McAfee:2018. 7)

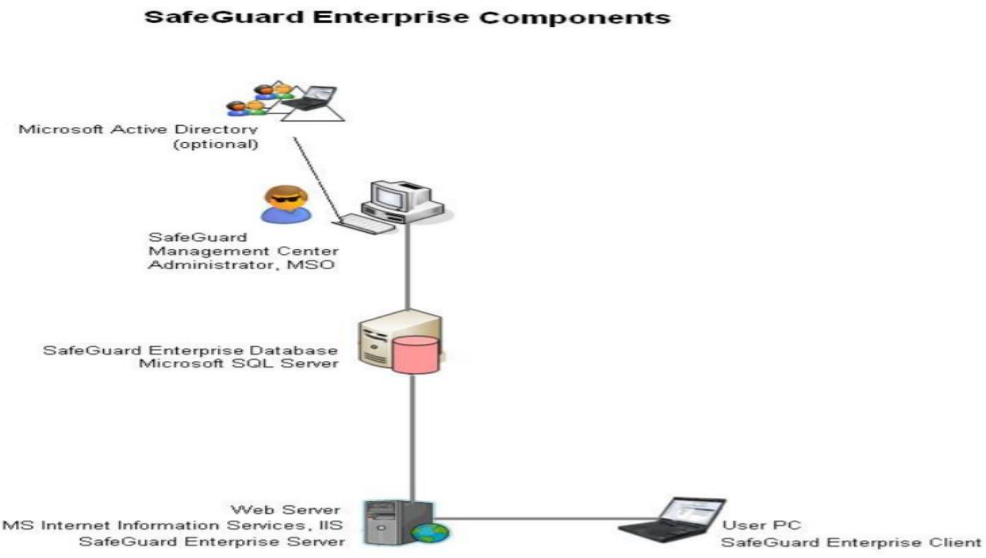
5.3.3. SafeGuard Enterprise

SafeGuard Enterprise, es una solución integral de seguridad de datos que utiliza una estrategia de cifrado basada en políticas para proporcionar protección de datos confiable en estaciones de trabajo, recursos compartidos de red y dispositivos móviles. Permite a los usuarios compartir información de forma segura y trabajar con archivos en dispositivos Windows, Mac OS X, iOS y Android con la ayuda de la aplicación Sophos Secure Workspace.

En SafeGuard Management Center, usted administra las políticas de seguridad, claves y certificados usando una estrategia de administración basada en roles. Los registros detallados y las funciones de informe garantizan que siempre tenga una visión general de todos los eventos.

Del lado del usuario, el cifrado de datos y la protección contra el acceso no autorizado son las principales funciones de seguridad de SafeGuard Enterprise. SafeGuard Enterprise se puede integrar perfectamente en el entorno normal del usuario. (Sophos, 2017).

Figura 10. Componentes Safeguard Enterprise.



Fuente: (Sophos, 2017)

Tabla 3. Descripción de los componentes individuales.

Componentes	Descripción
SafeGuard Enterprise Database(s) based on Microsoft SQL Server Database	Las bases de datos de SafeGuard Enterprise contienen todos los datos relevantes, como claves/certificados, información sobre usuarios y computadoras, eventos y Base de datos de SafeGuard Enterprise basada en la configuración de la política de base de datos de Microsoft SQL Server. La base de datos debe ser accedida por el servidor SafeGuard Enterprise Server y solo por un oficial de seguridad a través del Centro de gestión SafeGuard, generalmente el oficial de seguridad principal. Las bases de datos de SafeGuard Enterprise se pueden generar y configurar mediante un asistente o scripts.
SafeGuard Enterprise Server on IIS based web server	SafeGuard Enterprise Server se ejecuta como una aplicación en un IIS y permite la comunicación entre la base de datos SafeGuard Enterprise y el punto final SafeGuard Enterprise. A petición, SafeGuard Enterprise Server envía configuración de política a los puntos finales. Requiere .NET Framework 4.5 y ASP.NET 4.5. Cuando se elige SSL como método de cifrado de transporte para el cliente-servidor comunicación, la función de autenticación básica necesita ser instalada.
SafeGuard Management Center on administrator computer	Herramienta de administración central para puntos finales protegidos con SafeGuard Enterprise, usado para administrar claves y certificados, usuarios y computadoras, y para SafeGuard Management Center en la computadora del administrador que crea las políticas de SafeGuard Enterprise. El Centro de gestión de SafeGuard se comunica con la base de datos de SafeGuard Enterprise. Se requiere .NET Framework 4.5.
Directory Services (optional)	Importación de un Directorio Activo. Mantiene la organización de la compañía estructura con usuarios y computadoras.
SafeGuard Enterprise encryption software on endpoints	Software de cifrado para cifrado de datos y autenticación segura. Los puntos finales protegidos de SafeGuard Enterprise pueden conectarse a un servidor SafeGuard Enterprise (administrado) o no conectarse a un servidor SafeGuard Enterprise Server (no administrado). Los puntos finales administrados reciben sus políticas directamente del servidor de SafeGuard Enterprise. Los puntos finales no administrados reciben sus políticas dentro de paquetes de configuración que se pueden implementar utilizando mecanismos de distribución de terceros.

Fuente: (Sophos, 2017)

5.3.3.1. SafeGuard Full Disk Encryption

SafeGuard Full Disk Encryption con SafeGuard Power-on Authentication (POA) es el módulo de Sophos para cifrar volúmenes en puntos finales. Viene con una autenticación previa al arranque implementada por Sophos denominada SafeGuard Power-on Authentication (POA) que admite opciones de inicio de sesión como la tarjeta inteligente y la huella dactilar y un mecanismo de desafío / respuesta para la recuperación. (Sophos, 2017).

Los archivos se cifran de forma transparente. Cuando los usuarios abren, editan y guardan archivos, no se les solicita cifrado ni descifrado. Full Disk Encryption puede basarse en el volumen o archivo con diferentes claves y algoritmos. Como oficial de seguridad, usted especifica las configuraciones para el cifrado en una política de seguridad del tipo Protección de dispositivos.
SafeGuard Full Disk Encryption solo está disponible para los puntos finales del BIOS de Windows 7. Si usa Windows 7 UEFI o una versión más nueva de Windows, haga uso de la funcionalidad integrada de Windows BitLocker Drive Encryption. (Sophos, 2017).

5.3.3.1.1. Protege tus Macs

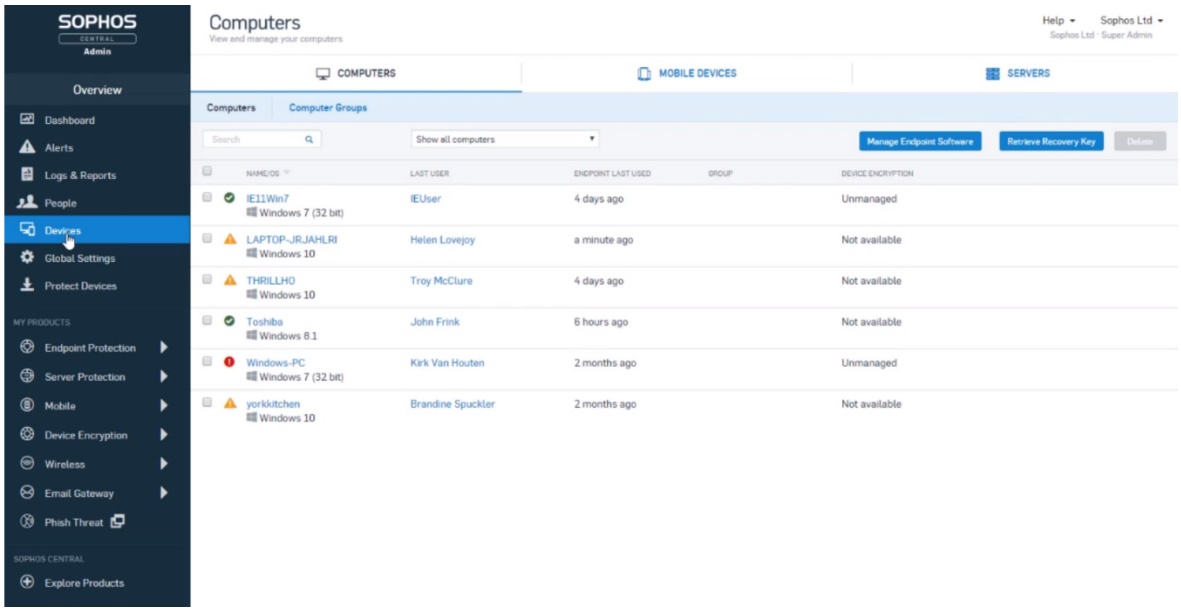
Los datos en una Mac son tan valiosos como los datos en una PC con Windows, lo que hace que sea vital incluir Macs en su estrategia de cifrado de datos. SafeGuard Enterprise protege sus Macs con encriptación de archivos y discos y asegura que los datos en sus Macs estén seguros en todo momento. Incluye la capacidad de cifrado para medios extraíbles, archivos compartidos de red y la nube en Mac. (Sophos, 2017).

- Administre el cifrado de archivos o discos para Mac en el mismo Centro de gestión que todos los demás dispositivos.
- Administrar dispositivos cifrados FileVault 2.
- Funciona en segundo plano sin afectar el rendimiento.
- Completa visibilidad e informes sobre el estado de cifrado.

5.3.3.1.2. Principales Beneficios

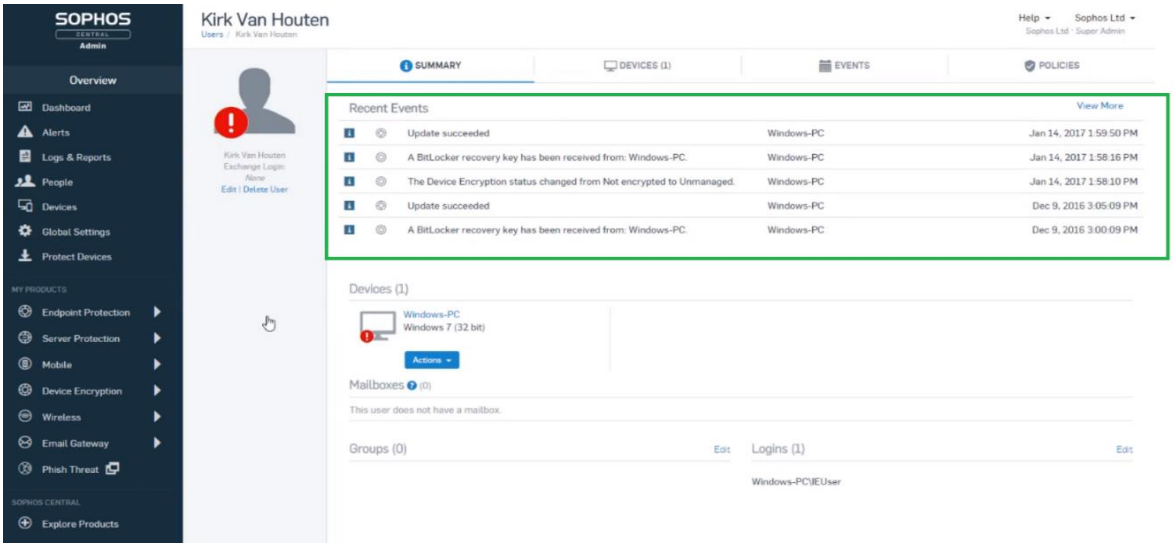
- **Evita fuga de información:** Proteja sus datos de forma inteligente contra robos, ataques, programas maliciosos y pérdidas accidentales de datos. Cifra el contenido de forma automática y este permanece cifrado incluso si se comparte o se carga a un sistema de intercambio de archivos en la nube.
- **Protección en tiempo real:** SafeGuard ofrece cifrado sincronizado gracias a la conexión de Sophos Endpoint Protection con Sophos Mobile Control. El agente local de SafeGuard escucha el "latido" de Security Heartbeat de un endpoint y habilita la protección proactiva automatizada.
- **Administre el cifrado completo de discos con Sophos Central:** La forma más fácil de administrar el cifrado completo de discos con BitLocker en Windows y FileVault en macOS es a través de Sophos Central Device Encryption. Permite configurar políticas en tres clics, no requiere instalar ningún servidor de administración de claves, incluye funciones de cumplimiento y creación de informes y ofrece recuperación de claves de autoservicio para sus usuarios. La instalación y la configuración se realizan en cuestión de minutos gracias a la intuitiva interfaz de administración basada en web de Sophos Central.
- **Cumplimiento, informes y administración:** Control simplificado y centralizado le ayuda a cumplir las normativas de protección de datos y evitar filtraciones.

Figura 11. Consola central Sophos.



Fuente: (Sophos, 2017)

Figura 12. Consola central Sophos.



Fuente: (Sophos, 2017)

5.3.4. VeraCrypt

VeraCrypt es un software gratuito de cifrado de disco de código abierto para Windows, Mac OSX y Linux. Presentado por **IDRIX** (https://www.idrix.fr) y basado en TrueCrypt 7.1a.

VeraCrypt es un software para establecer y mantener un volumen cifrado sobre la marcha (dispositivo de almacenamiento de datos). El cifrado sobre la marcha significa que los datos se cifran automáticamente justo antes de guardarlos y descifrarlos inmediatamente después de que se carguen, sin intervención del usuario. No se pueden leer (descifrar) los datos almacenados en un volumen cifrado sin utilizar la contraseña / archivo clave correctos o las claves de cifrado correctas. Todo el sistema de archivos está encriptado (por ejemplo, nombres de archivos, nombres de carpetas, contenido de cada archivo, espacio libre, metadatos, etc.). (Veracrypt, 2018).

5.3.4.1. Características principales de VeraCrypt

- Crea un disco encriptado virtual dentro de un archivo y lo monta como un disco real.
- Encripta una partición completa o dispositivo de almacenamiento como unidad flash USB o disco duro.
- Encripta una partición o unidad donde está instalado Windows (autenticación previa al inicio).
- La paralelización y la canalización permiten que los datos se lean y escriban tan rápido como si la unidad no estuviera encriptada.
- El cifrado puede acelerarse por hardware en procesadores modernos.

- Proporciona una negación plausible, en caso de que un adversario te obligue a revelar la contraseña: volumen oculto (esteganografía) y sistema operativo oculto.

¿Qué te trae VeraCrypt?

VeraCrypt agrega seguridad mejorada a los algoritmos utilizados para el cifrado de sistemas y particiones, lo que lo hace inmune a los nuevos desarrollos en ataques de fuerza bruta. VeraCrypt también resuelve muchas vulnerabilidades y problemas de seguridad que se encuentran en TrueCrypt.
Como ejemplo, cuando la partición del sistema está encriptada, TrueCrypt usa PBKDF2-RIPEMD160 con 1,000 iteraciones, mientras que en VeraCrypt usamos 327,661. Y para contenedores estándar y otras particiones, TrueCrypt usa como máximo 2,000 iteraciones, pero VeraCrypt usa 655,331 para RIPEMD160 y 500,000 iteraciones para SHA-2 y Whirlpool. (Veracrypt, 2018).

Esta seguridad mejorada agrega algo de retraso solo a la apertura de particiones cifradas sin ningún impacto en el rendimiento de la fase de uso de la aplicación. Esto es aceptable para el propietario legítimo, pero hace que sea mucho más difícil para un atacante obtener acceso a los datos cifrados. (Veracrypt, 2018).

A partir de la versión 1.12, es posible utilizar iteraciones personalizadas a través de la función PIM, que se puede usar para aumentar la seguridad del cifrado.
A partir de la versión 1.0f, VeraCrypt puede cargar el volumen de TrueCrypt. También ofrece la posibilidad de convertir contenedores TrueCrypt y particiones que no sean del sistema al formato VeraCrypt. (Veracrypt, 2018).

Actualización 12 de septiembre de 2018: VeraCrypt 1.23 ha sido lanzado. Ofrece mejoras para el cifrado del sistema EFI de Windows, como la

compatibilidad con SecureBoot predeterminado. También soluciona algunos problemas y agrega algunas características.

Actualización 30 de marzo de 2018: VeraCrypt 1.22 ha sido lanzado. Soluciona muchos problemas y trae algunas mejoras y características (por ejemplo, aceleración de Kuznyechik, nuevos algoritmos de cifrado en cascadas y compatibilidad con TRIM para SSD).

Actualización 9 de julio de 2017: VeraCrypt 1.21 ha sido lanzado. Corrige muchas regresiones encontradas en la versión 1.20 y trae soporte para FreeBSD. Se insta a todos los usuarios a actualizar a esta nueva versión.

Actualización 29 de junio de 2017: VeraCrypt 1.20 ha sido lanzado. Trae correcciones de errores, mejoras de rendimiento y nuevas características. También es la primera versión que incluye documentación HTML local en lugar del PDF habitual de la Guía del usuario.

Actualización 17 de octubre de 2016: VeraCrypt 1.19 ha sido lanzado. Incluye soluciones para problemas informados por la auditoría de Quarkslab que fue financiado por OSTIF. Esta versión también trae muchas mejoras y correcciones, como la aceleración del algoritmo Serpent por un factor de 2.5 y la compatibilidad de Windows 32 bits para el cifrado del sistema EFI. Por favor, consulte las notas de la versión para ver la lista completa de cambios.

Actualización 18 de agosto de 2016: el instalador de Windows para VeraCrypt 1.18 se ha actualizado para incluir los controladores firmados por Microsoft que permiten que VeraCrypt se ejecute en Windows 10 Anniversary Edition. La versión de Windows Installer se incrementó a 1.18a pero no se modificó en el nivel de VeraCrypt. Los instaladores Linux y MacOSX permanecen sin cambios.

Actualización 17 de agosto de 2016: VeraCrypt 1.18 ha sido lanzado. Proporciona el cifrado del sistema EFI para Windows (una primicia mundial en la comunidad de código abierto) y resuelve una vulnerabilidad TrueCrypt que permite al atacante detectar la presencia de volumen oculto. Esta versión también trae muchas mejoras y correcciones.

5.3.4.2. Encriptación del sistema

VeraCrypt puede encriptar una partición del sistema o una unidad de sistema completa, es decir, una partición o unidad donde está instalado Windows y desde donde arranca.

El cifrado del sistema proporciona el más alto nivel de seguridad y privacidad, porque todos los archivos, incluidos los archivos temporales que Windows y las aplicaciones crean en la partición del sistema (normalmente sin su conocimiento o consentimiento), archivos de hibernación, archivos de intercambio, etc., son siempre permanentes encriptado (incluso cuando la fuente de alimentación se interrumpe repentinamente). Windows también registra grandes cantidades de datos potencialmente confidenciales, como los nombres y las ubicaciones de los archivos que abre, las aplicaciones que ejecuta, etc. Todos los archivos de registro y las entradas de registro siempre se encriptan permanentemente. (Veracrypt, 2018).

El cifrado del sistema implica la autenticación previa al inicio, lo que significa que cualquier persona que desee obtener acceso y usar el sistema encriptado, leer y escribir archivos almacenados en la unidad del sistema, etc., deberá ingresar la contraseña correcta cada vez antes de que Windows arranque. La autenticación previa al inicio se maneja con VeraCrypt Boot Loader, que reside en la primera pista de la unidad de arranque y en el disco de rescate de VeraCrypt. (Veracrypt, 2018).

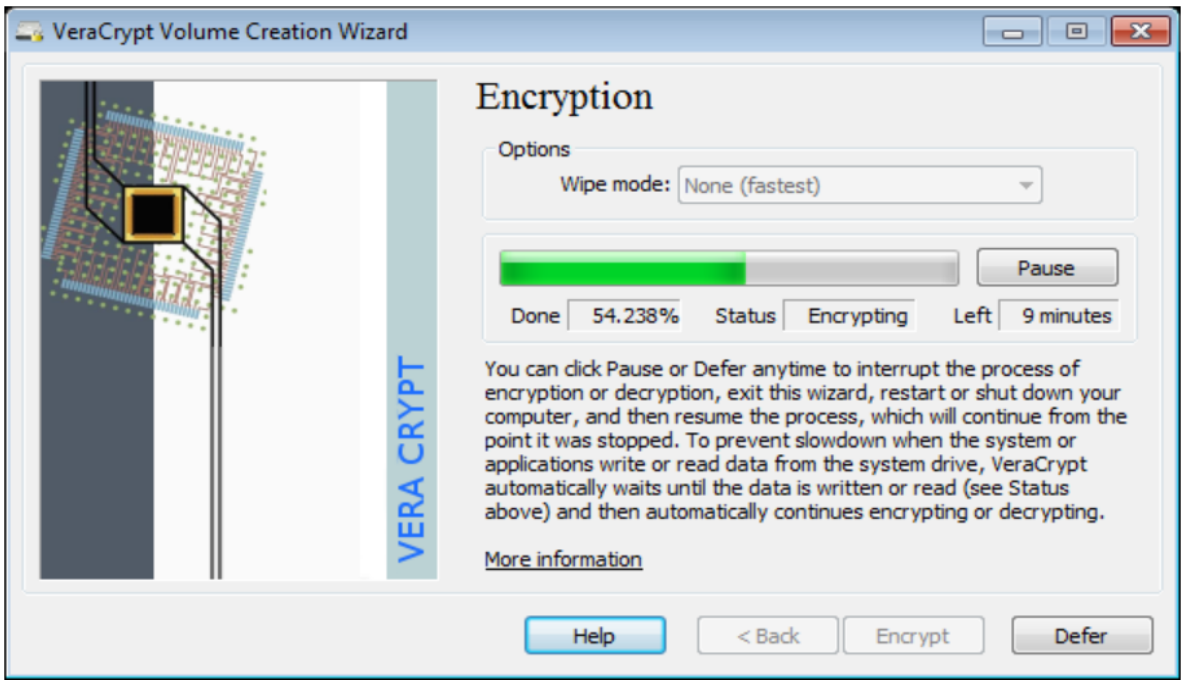
Tenga en cuenta que VeraCrypt puede encriptar una partición / unidad de sistema no encriptada existente mientras el sistema operativo se está ejecutando (mientras el sistema está siendo encriptado, puede usar su computadora como de costumbre sin ninguna restricción). Del mismo modo, una partición / unidad del sistema encriptada con VeraCrypt se puede descifrar en el lugar mientras se está

ejecutando el sistema operativo. Puede interrumpir el proceso de cifrado o descifrado en cualquier momento, dejar la partición / unidad parcialmente desencriptada, reiniciar o apagar la computadora, y luego reanudar el proceso, que continuará desde el momento en que se detuvo. (Veracrypt, 2018).
Para cifrar una partición del sistema o una unidad de sistema completa, seleccione **Sistema > Encriptar partición / unidad del sistema y luego siga las instrucciones en el asistente.** Para **descifrar una partición / unidad del sistema, seleccione Sistema > Descifrar permanentemente partición / unidad del sistema.**

Debido a los requisitos de BIOS, la contraseña previa al inicio se escribe utilizando el diseño de teclado de EE. UU. Durante el proceso de encriptación del sistema, VeraCrypt automáticamente y de forma transparente cambia el teclado a la disposición de los EE. UU. Para garantizar que el valor de la contraseña ingresada coincida con el que se escribió en el modo previo al inicio. Por lo tanto, para evitar errores de contraseña incorrectos, se debe escribir la contraseña usando las mismas claves que cuando se crea el cifrado del sistema. (Veracrypt, 2018).

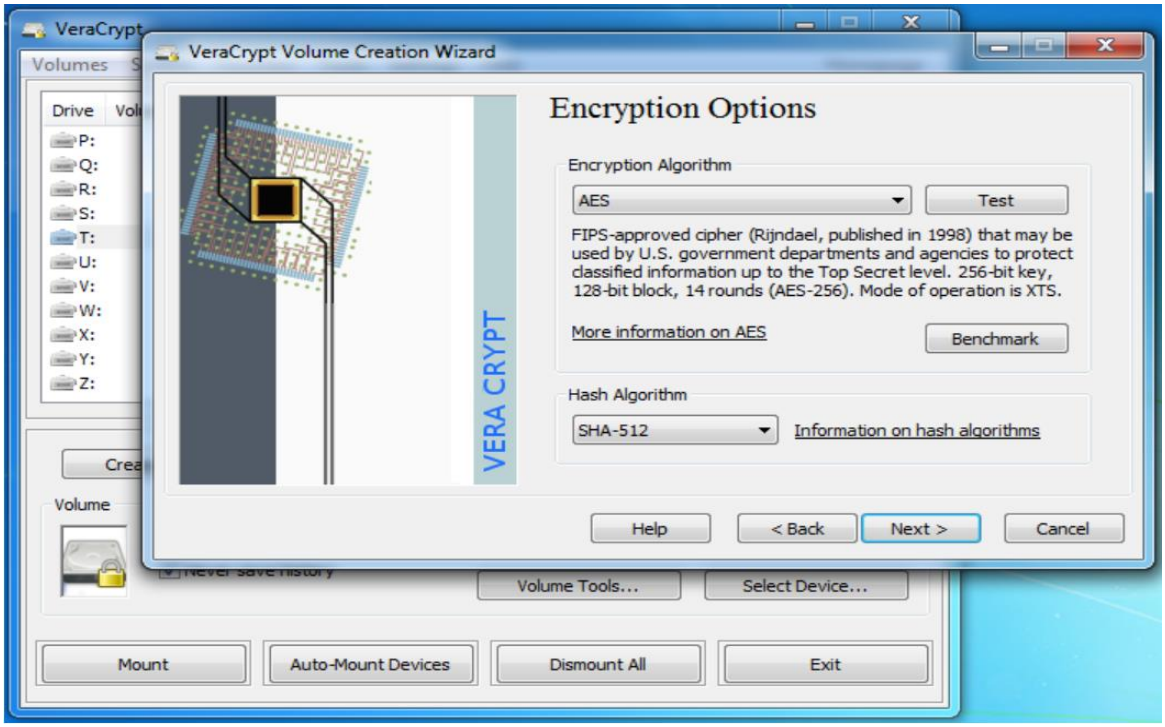
Nota: de forma predeterminada, Windows 7 y versiones posteriores arrancan desde una partición especial pequeña. La partición contiene archivos que son necesarios para arrancar el sistema. Windows solo permite que las aplicaciones que tienen privilegios de administrador escriban en la partición (cuando el sistema se está ejecutando). VeraCrypt encripta la partición solo si elige cifrar toda la unidad del sistema (en lugar de elegir encriptar solo la partición donde está instalado Windows). (Veracrypt, 2018).

Imagen 13. Encriptando la partición del sistema.



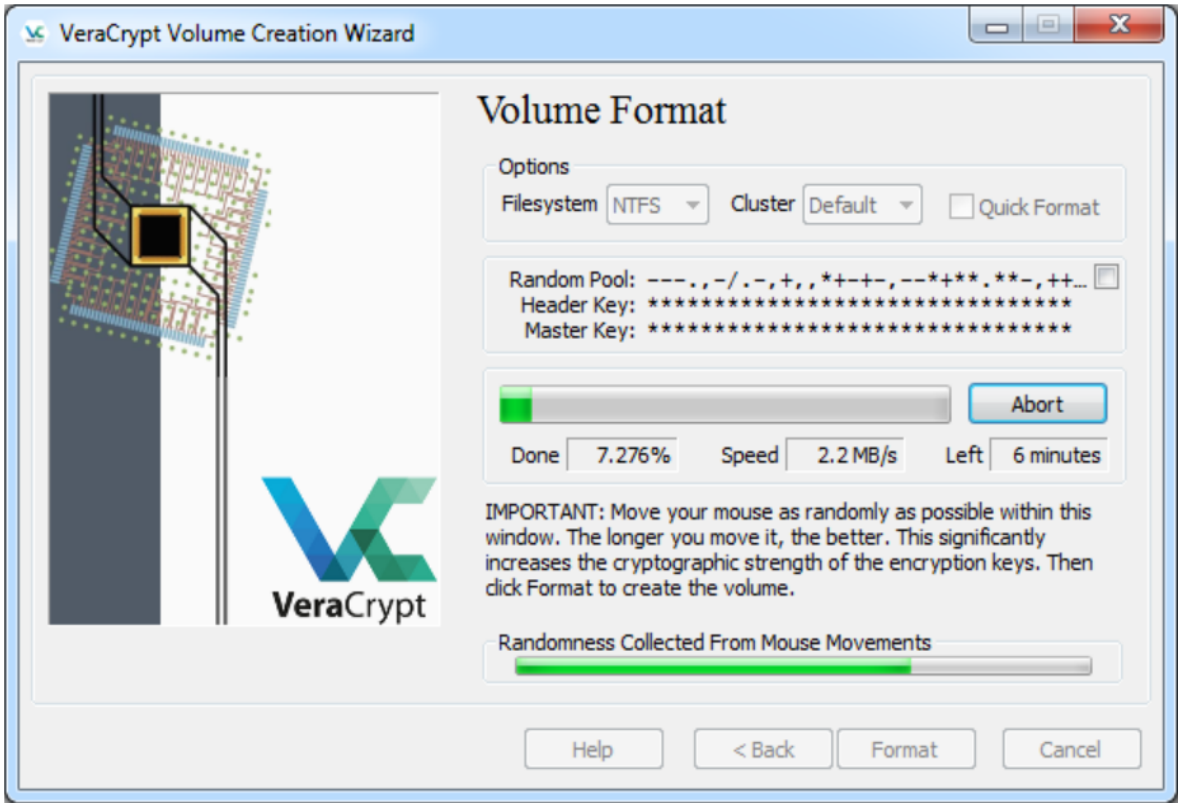
Fuente: (Elaboración propia)

Imagen 14. Creando un volumen encriptado.



Fuente: (Elaboración propia)

Imagen 15. Formateo de Volumen creado en la imagen anterior.



Fuente: (Elaboración propia)

5.3.5. BitLocker

Cifrado de unidad BitLocker es una característica de protección de datos que se integra en el sistema operativo y soluciona las amenazas de robo o exposición de datos de equipos perdidos, sustraídos o retirados inadecuadamente.

BitLocker ofrece la máxima protección cuando se usa con un módulo de plataforma segura (TPM) 1.2 o posterior. El TPM es un componente de hardware instalado en muchos equipos nuevos por los fabricantes de equipos. Funciona con BitLocker para ayudar a proteger los datos de usuario y para garantizar que un equipo no se haya manipulado mientras el sistema estaba sin conexión. (Microsoft, 2015).

En los equipos que no tienen un TPM versión 1.2 o posterior, todavía puede usar BitLocker para cifrar la unidad del sistema operativo Windows. Sin embargo, esta implementación requerirá que el usuario inserte una clave de inicio USB para iniciar el equipo o reanudarlo del modo de hibernación. A partir de Windows 8, puedes usar una contraseña de volumen del sistema operativo para proteger el volumen del sistema operativo en un equipo sin TPM. Ambas opciones no proporcionan la comprobación de integridad del sistema previa al inicio ofrecida por BitLocker con un TPM. (Microsoft, 2015).

Además del TPM, BitLocker ofrece la opción de bloquear el proceso de inicio normal hasta que el usuario proporcione un número de identificación personal (PIN) o inserte un dispositivo extraíble, como una unidad flash USB, que contenga una clave de inicio. Estas medidas de seguridad adicionales proporcionan autenticación multifactor y la garantía de que el equipo no se inicia o reanuda desde la hibernación hasta que se ofrezca el PIN o la clave de inicio correctos. (Microsoft, 2015).

5.3.5.1. Aplicaciones prácticas

Los datos de un equipo perdido o robado son vulnerables a un acceso no autorizado, mediante la ejecución de una herramienta de ataques de software contra ellos o mediante la transferencia del disco duro del equipo a otro equipo. BitLocker ayuda a mitigar el acceso a datos no autorizados mejorando las protecciones de archivo y de sistema. BitLocker también ayuda a convertir los datos en inaccesibles cuando se retiran o reciclan equipos protegidos con BitLocker. (Microsoft, 2015).

Hay dos herramientas adicionales en las herramientas de administración remota del servidor, que puedes usar para administrar BitLocker.

- **Visor de contraseñas de recuperación de BitLocker**. El Visor de contraseñas de recuperación de BitLocker te permite buscar y ver las contraseñas de recuperación de cifrado de unidad BitLocker a las que se haya hecho una copia de seguridad en los servicios de dominio de Active Directory (AD DS). Puedes usar esta herramienta para ayudar a recuperar datos que están almacenados en una unidad cifrada mediante el uso de BitLocker. La herramienta Visor de contraseñas de recuperación de BitLocker es una extensión del complemento Microsoft Management Console (MMC) de Usuarios y equipos de Active Directory.

  Con esta herramienta, puedes examinar el cuadro de diálogo **Propiedades** de un objeto del equipo para ver las contraseñas de recuperación de BitLocker correspondientes. Además, puedes hacer clic con el botón derecho en un contenedor de dominio y, a continuación, buscar una contraseña de recuperación de BitLocker en todos los dominios del bosque de Active Directory. Para ver las contraseñas de recuperación, debes ser un administrador de dominio o debes tener delegados los permisos de administrador de dominio.

- **Herramientas de cifrado de unidad BitLocker**. Las herramientas de cifrado de unidad BitLocker incluyen las herramientas de línea de comandos manage-bde y repair-bde, y los cmdlets de BitLocker para Windows PowerShell. Tanto manage-bde como los cmdlets de BitLocker pueden usarse para realizar cualquier tarea procesable a través del panel de control de BitLocker y son adecuados para implementaciones automatizadas y otros escenarios de scripts. Repair-bde se proporciona para escenarios de recuperación ante desastres en los que una unidad protegida con BitLocker no se puede desbloquear con normalidad o mediante la consola de recuperación.

5.3.5.2. Nuevas funciones en Windows 10, versión 1511

Algoritmo de cifrado XTS-AES. BitLocker ahora es compatible con el algoritmo de cifrado XTS-AES. XTS-AES proporciona protección adicional de un tipo de ataques de cifrado que se basan en la manipulación de texto cifrado para provocar cambios predecibles en texto sin formato. BitLocker admite las claves de XTS-AES de 128 bits y de 256 bits.

Aporta los siguientes beneficios:

- El algoritmo es compatible con FIPS.
- Fácil de administrar. Puedes usar el asistente para BitLocker, manage-bde, la directiva de grupo, la directiva MDM, Windows PowerShell o WMI para administrarlo en dispositivos de tu organización.

Nota: No podrás acceder a las unidades cifradas con XTS-AES en versiones anteriores de Windows. Se recomienda únicamente para unidades fijas y de sistema operativo. Las unidades extraíbles deben seguir usando los algoritmos AES-CBC de 128 bits o AES-CBC 256 bits. (Microsoft, 2015).

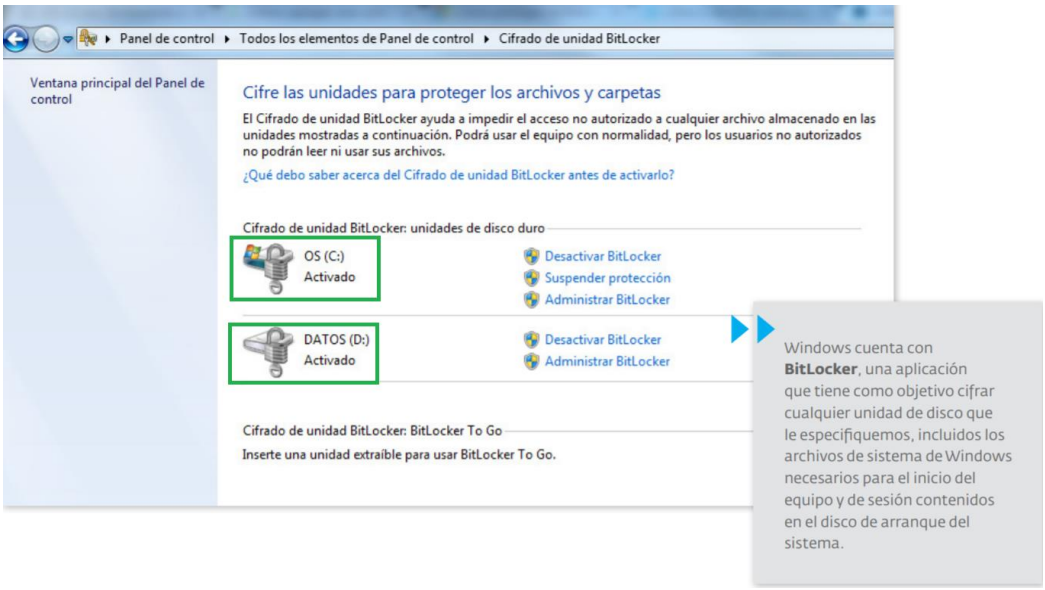
5.3.5.3. Nuevas funciones en Windows 10

- **Cifrar y recuperar tu dispositivo con Azure Active Directory**. Además de usar una cuenta de Microsoft, el cifrado de dispositivo automático ahora puede cifrar los dispositivos que están unidos a un dominio de Azure Active Directory. Cuando el dispositivo está cifrado, la clave de recuperación de BitLocker queda automáticamente custodiada para Azure Active Directory. De esta forma, será más fácil recuperar la clave de BitLocker en línea.

- **Protección de puerto DMA**. Puedes usar la directiva MDM DataProtection/AllowDirectMemoryAccess para bloquear puertos DMA cuando el dispositivo se está iniciando. Además, cuando un dispositivo está bloqueado, se desactivan todos los puertos DMA que no están en uso, aunque todos los dispositivos que ya están conectados a un puerto DMA seguirán funcionando. Cuando el dispositivo esté desbloqueado, todos los puertos DMA se vuelven a activar.

- **Nueva directiva de grupo para configurar la recuperación de prearranque**. Ahora puedes configurar el mensaje de recuperación de prearranque y recuperar la dirección URL que se muestra en la pantalla de recuperación de prearranque.

Imagen 16. BitLocker activado en C y D.



Fuente: (Elaboración propia)

5.3.5.4. Requisitos del sistema

BitLocker tiene los siguientes requisitos de hardware:

Para que BitLocker use la comprobación de integridad del sistema proporcionada por un módulo de plataforma segura (TPM), el equipo debe tener TPM 1.2 o posterior. Si el equipo no tiene un TPM, la habilitación de BitLocker requiere que guardes una clave de inicio en un dispositivo extraíble, como una unidad flash USB. (Microsoft, 2015).

Un equipo con un TPM también debe tener un firmware de BIOS o UEFI compatible con Trusted Computing Group (TCG). El firmware de BIOS o UEFI establece una cadena de confianza para el inicio del sistema preoperativo, y debe incluir compatibilidad con la raíz estática de Trust Measurement especificada por TCG. Un equipo sin un TPM no requiere firmware compatible con TCG. (Microsoft, 2015).

El firmware de BIOS o UEFI del sistema (para equipos TPM y no TPM) debe admitir la clase de dispositivo de almacenamiento masivo USB, lo que incluye la lectura de pequeños archivos de una unidad flash USB en el entorno de sistema preoperativo. (Microsoft, 2015).

El disco duro debe particionarse con al menos dos unidades:

- La unidad del sistema operativo (o la unidad de arranque) contiene el sistema operativo y sus archivos de compatibilidad. Debe estar formateada con el sistema de archivos NTFS. (Microsoft, 2015).
- La unidad del sistema contiene los archivos que son necesarios para cargar Windows después de que el firmware haya preparado el hardware del sistema. BitLocker no está habilitado en esta unidad. Para que funcione BitLocker, la unidad del sistema no debe estar cifrada, debe ser diferente de la unidad del sistema operativo y debe estar formateada con el sistema de archivos FAT32 en equipos que usan firmware basado en UEFI o con el sistema de archivos NTFS en equipos que usan firmware BIOS. Recomendamos que la unidad del sistema tenga un tamaño aproximado de 350 MB. Una vez activado BitLocker, debe tener aproximadamente 250 MB de espacio libre. (Microsoft, 2015).

Cuando se instala en un equipo nuevo, Windows crea automáticamente las particiones que son necesarias para BitLocker.
Cuando se instala el componente opcional de BitLocker en un servidor también deberás instalar la característica de almacenamiento mejorado, que se usa para admitir unidades cifradas de hardware. (Microsoft, 2015).

5.4. Análisis de aplicaciones de cifrado de disco completo

Al concluir el análisis de las cuatro aplicaciones de cifrado basándonos en el cuadrante mágico de Gartner, en la tabla 4 se realizó una comparación con las principales características de cada una de las aplicaciones, podemos decir que la aplicación Veracrypt y Bitlocker no aplican para la implementación en la UCN, porque no poseen una gestión centralizada y no la podemos integrar con el directorio activo, esto hace mucho más complicado la administración, estas aplicaciones son muy funcional cuando son pocos dispositivos a implementar.

Las otras dos aplicaciones, McAfee Drive Encryption y SafeGuard Enterprise si cumplen con una gestión centralizada y se pueden integrar con el directorio activo, a través de esta gestión se hace mucho más fácil la administración de los dispositivos portátiles, aplicándoles diferentes políticas de seguridad para proteger el acceso a la información contenido en los discos duros, las características de ambas aplicaciones son muy similares. Para realizar la selección entre estas dos aplicaciones, en la tabla 5 se realizó una comparación entre las cotizaciones a nivel de los costos para 100 licencias para la implementación, es mucho más favorable la solución de McAfee porque es 455.40 dólares americanos más barata respecto a la solución de SafeGuard. Además, la aplicación de cifrado de McAfee incluye productos adicionales que se pueden implementar en un futuro y no tendrían costos adicionales.

Tabla 4. Comparación de aplicaciones de cifrado.

Soluciones	Licencia	Empresa	Consola Admon.	Algoritmo	Integración LDAP	Sistema Operativo Servidor	Sistema Operativo Cliente
McAfee Drive Encryption	Comercial Licencia por host	McAfee	Si	AES 256	Si	Windows Server 2008 SP2, Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 SP2, Windows Server 2016.	Windows 7 SP1, Windows 8.1, Windows 10
SafeGuard Enterprise	Comercial Licencia por host	Sophos	Si	AES 256	Si	Windows Server 2008 SP2, Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 SP2, Windows Server 2016.	Windows 7 SP1, Windows 8.1, Windows 10
VeraCrypt	Open	IDRIX	No	AES 256	No	No Aplica	Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows 8.1, Windows 10
BitLocker	Comercial Licencia por host	Windows	No		No	No Aplica	Windows 7, Windows 8, Windows 8.1, Windows 10

Fuente: (Elaboración propia)

Tabla 5. Comparación de Precio

INTELECTOR				SENCOM		
Descripción	**Cantidad**	**Precio Unitario**	**Total**	**Descripción**	**Precio Unitario**	**Total**
SafeGuard Disk Encryption Advanced, Includes: SafeGuard Device Encryption, SafeGuard Native Device Encryption, Management Center, Suscripción 1 año.	100	$26.34	$2,634.00	MFE Complete EP Bus P:1 BZ [P+]CompUPGD 100 Licencias	$22.38	$2,238.00
Instalación y configuración.	1	$0.00	$0.00	Servicios de Asistencia y Soporte Técnico en administración de la solución, durante la vigencia de licencia.	$0.00	$0.00
-	-	Sub Total	$2,634.00	-	Sub Total	$2,238.00
		Iva	$395.10		Iva	$335.70
		Total	**$3,029.10**		**Total**	**$2,573.70**

Fuente: (Elaboración propia)

6. Análisis y presentación de resultados

Al implementar el proyecto de un sistema para proteger la información confidencial en dispositivos portátiles en la Universidad Central de Nicaragua, se mitiga en un 99% que la información contenida en sus discos duros sea accesible únicamente por personal autorizado, en caso de robo o pérdida de estos dispositivos portátiles, no es posible ingresar al disco duro para acceder a la información. En caso que retiren el disco y lo conecten a otro dispositivo, la información estará ilegible, incluso aun implementando numerosas técnicas para desencriptar la información, para poder utilizar el disco duro es necesario formatearlo y la información se pierde, no es posible recuperarla por ningún medio.

En caso de que un dispositivo portátil sufra daños de hardware, pero el disco duro se encuentra en buen estado, existen métodos propios de la solución para recuperar la información, siempre y cuando se tenga acceso a la consola de administración del servidor de cifrado.

6.1. Metodología

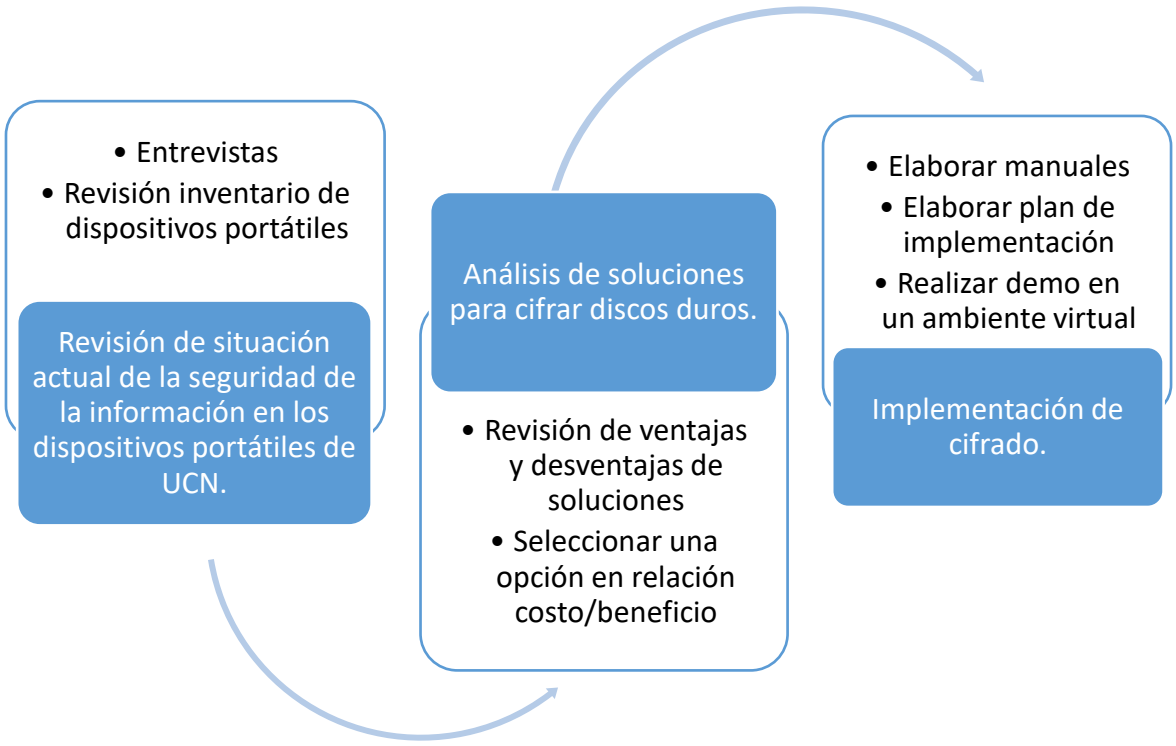
El proyecto de implementación de un sistema de protección de la información confidencial en dispositivos portátiles de la Universidad Central de Nicaragua inició con la revisión de la situación actual de la seguridad de la información en los dispositivos portátiles, se analizaron cuatro opciones del mercado basado en el cuadrante mágico de Gartne, la selección se realizó en cuando a costo-beneficio, funcionalidades y según las necesidades de la UCN.

Esta solución se integra con un servidor de directorio activo existente, cuenta con una gestión centralizada de todos los dispositivos y además en un

futuro se puede ir implementando la integración de nuevos productos, para reforzar la protección de la información en la universidad.

En resumen, la metodología que se llevó a cabo en la Universidad Central de Nicaragua, se puede apreciar en la figura 17, que se detalla a continuación.

Figura 17. Metodología utilizada.



Fuente: (Elaboración propia)

6.2. Revisión de situación actual de la seguridad de la información en los dispositivos portátiles de UCN.

La Universidad Central de Nicaragua cuenta con 4 recintos a nivel nacional, que se listan a continuación:

1. Campus Central (Managua).
2. Campus Doral (Managua).
3. Campus Jinotepe.
4. Recinto Estelí.

Actualmente la Universidad Central de Nicaragua tiene un inventario total de 100 dispositivos portátiles a nivel nacional, distribuidas de la siguiente manera:

- El Campus Central (Managua) cuenta con 55 dispositivos portátiles.
- El Campus Doral (Managua) cuenta con 25 dispositivos portátiles
- El Campus Jinotepe cuenta con 10 dispositivos portátiles.
- El Recinto Estelí cuenta con 10 dispositivos portátiles.

La UCN no cuenta con una solución para proteger la información contenida en sus discos duros, en caso de pérdida o robo de estos dispositivos, la información puede ser manipulada y usada por personal no autorizado.
Se realizó una demostración muy sencilla, esta consistió en retirar un disco duro de uno de los dispositivos y conectarlo en un case externo USB (enclosure), se conectó en otro dispositivo, se corroboró que la información contenida en este disco duro podía manipularse sin problemas.
Se pudo corroborar que, en años anteriores en la UCN, ha tenido varios incidentes de pérdidas de dispositivos portátiles, la información contenida en estos dispositivos no se encontraba protegida y aquí la gran necesidad de implementar una solución para proteger esta información.

6.3. Plan de Implementación de McAfee Drive Encryption.

Para la implementación de McAfee Drive Encryption en la Universidad Nacional de Nicaragua, se revisó la infraestructura actual y se cuenta con un ambiente virtual (Servidor de directorio activo, BD, etc.), para esta implementación es necesario únicamente crear un nuevo servidor virtual para la instalación y configuración de consola, como se puede apreciar en la imagen 19 y agregar en el firewall permisos puntuales a las redes de las 4 sucursales de la UCN para que exista comunicación con el nuevo servidor de consola Epo McAfee, como se puede apreciar en la tabla 7.

El sistema operativo a utilizar en este nuevo servidor, es un Windows Server 2012 R2 que la UCN cuenta con licencia y una base de datos con SQL Express 2012. Los requerimientos de hardware son los mínimos recomendados por la solución de McAfee Drive Encryption.

Tabla 6. Redes y puertos de Sucursales

Sucursal	Redes	Servidor McAfee	Puertos
Campus Central	192.168.1.0/24	10.11.0.11	80
Campus Central	192.168.1.0/24	10.11.0.11	8443
Campus Central	192.168.1.0/24	10.11.0.11	8444
Campus Doral	192.168.2.0/24	10.11.0.11	80
Campus Doral	192.168.2.0/24	10.11.0.11	8443
Campus Doral	192.168.2.0/24	10.11.0.11	8444
Campus Jinotepe	192.168.3.0/24	10.11.0.11	80
Campus Jinotepe	192.168.3.0/24	10.11.0.11	8443
Campus Jinotepe	192.168.3.0/24	10.11.0.11	8444
Recinto Estelí	192.168.4.0/24	10.11.0.11	80
Recinto Estelí	192.168.4.0/24	10.11.0.11	8443
Recinto Estelí	192.168.4.0/24	10.11.0.11	8444

Fuente: (Elaboración propia)

Tabla 7. ACL's a aplicar en Firewall

Sucursal	ACL's
Campus Central	access-list 50 permit tcp 192.168.1.0 0.0.0.255 10.11.0.11 0.0.0.0 eq 80
Campus Central	access-list 50 permit tcp 192.168.1.0 0.0.0.255 10.11.0.11 0.0.0.0 eq 8443
Campus Central	access-list 50 permit tcp 192.168.1.0 0.0.0.255 10.11.0.11 0.0.0.0 eq 8444
Campus Doral	access-list 50 permit tcp 192.168.2.0 0.0.0.255 10.11.0.11 0.0.0.0 eq 80
Campus Doral	access-list 50 permit tcp 192.168.2.0 0.0.0.255 10.11.0.11 0.0.0.0 eq 8443
Campus Doral	access-list 50 permit tcp 192.168.2.0 0.0.0.255 10.11.0.11 0.0.0.0 eq 8444
Campus Jinotepe	access-list 50 permit tcp 192.168.3.0 0.0.0.255 10.11.0.11 0.0.0.0 eq 80
Campus Jinotepe	access-list 50 permit tcp 192.168.3.0 0.0.0.255 10.11.0.11 0.0.0.0 eq 8443
Campus Jinotepe	access-list 50 permit tcp 192.168.3.0 0.0.0.255 10.11.0.11 0.0.0.0 eq 8444
Recinto Estelí	access-list 50 permit tcp 192.168.4.0 0.0.0.255 10.11.0.11 0.0.0.0 eq 80
Recinto Estelí	access-list 50 permit tcp 192.168.4.0 0.0.0.255 10.11.0.11 0.0.0.0 eq 8443
Recinto Estelí	access-list 50 permit tcp 192.168.4.0 0.0.0.255 10.11.0.11 0.0.0.0 eq 8444

Fuente: (Elaboración propia)

Tabla 8. Descripción de puertos que se permiten en firewall

Puerto	Predeterminado	Descripción	Dirección del tráfico
Puerto de comunicación agente-servidor	80	Puerto TCP que el servicio del servidor de ePO usa para recibir solicitudes de agentes.	Conexión entrante al controlador de agentes y el servidor de ePO desde McAfee Agent. Conexión entrante al servidor de ePO desde el controlador de agentes remoto.
Puerto de comunicación consola-servidor de aplicaciones	8443	Puerto TCP que el servicio del servidor de aplicaciones de ePO usa para permitir el acceso de la IU al navegador web.	Conexión entrante al servidor de ePO desde la consola de ePO.
Puerto de comunicación autenticada cliente-servidor	8444	Puerto TCP que el controlador de agentes usa para comunicarse con el servidor de ePO con el fin de obtener información requerida (por ejemplo, servidores LDAP).	Conexión saliente desde los controladores remotos al servidor de ePO.

Fuente: (McAfee, 2018)

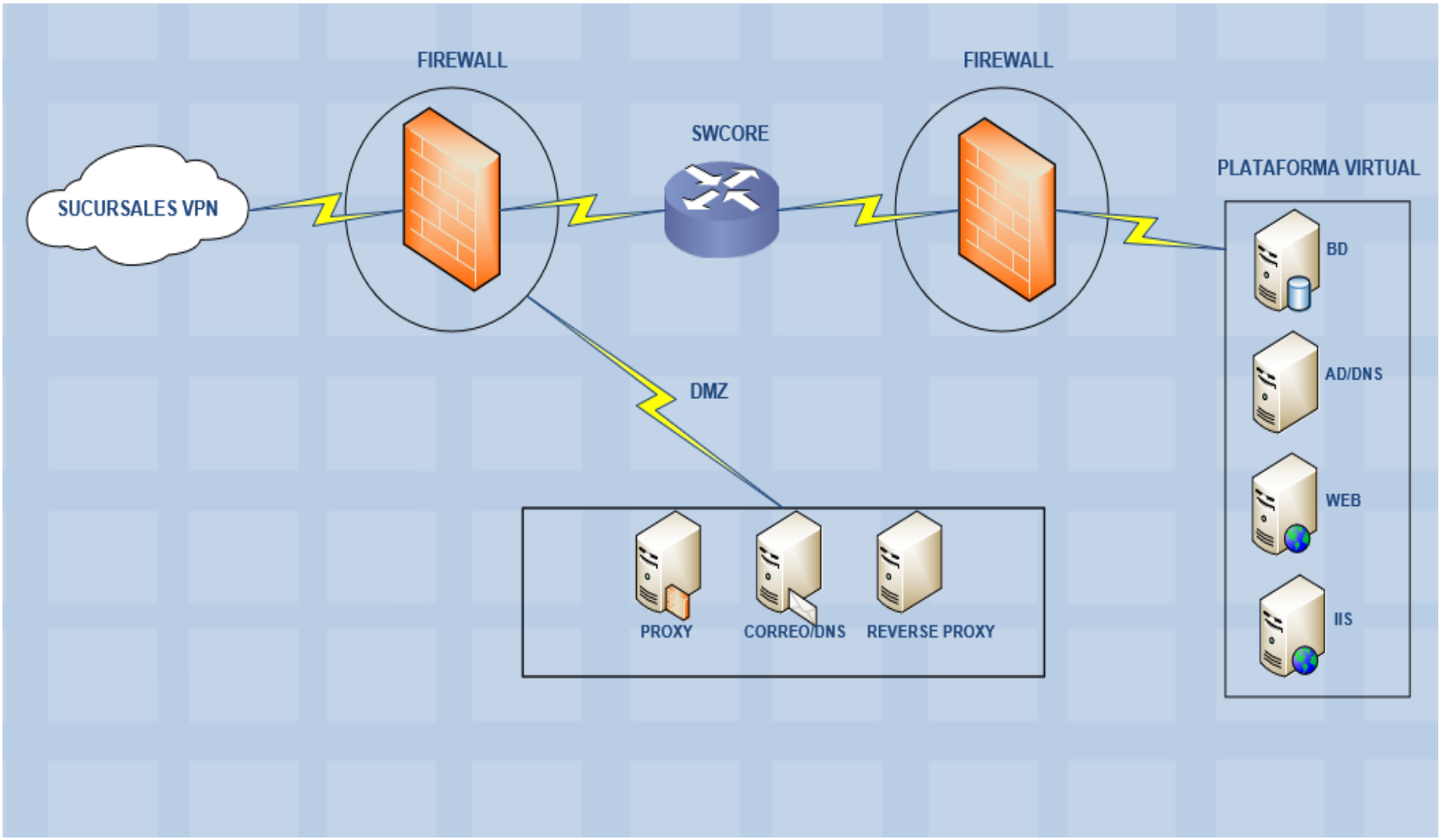
En el filtro de contenido es necesario que se de acceso a los puertos y url que se describen en la tabla 9 que se muestra a continuación.

Tabla 9. Actualizaciones de McAfee.

Puerto predeterminado	Protocolo	Dirección del tráfico
21	TCP	Conexión saliente desde el servidor de ePO a ftp://ftp.nai.com
80	TCP	Conexión saliente desde el servidor de ePO a http://update.nai.com
443	TCP	Conexión saliente desde el servidor de ePO a s-download.mcafee.com y epo.mcafee.com NOTA: Estas direcciones URL no son accesibles desde navegadores.

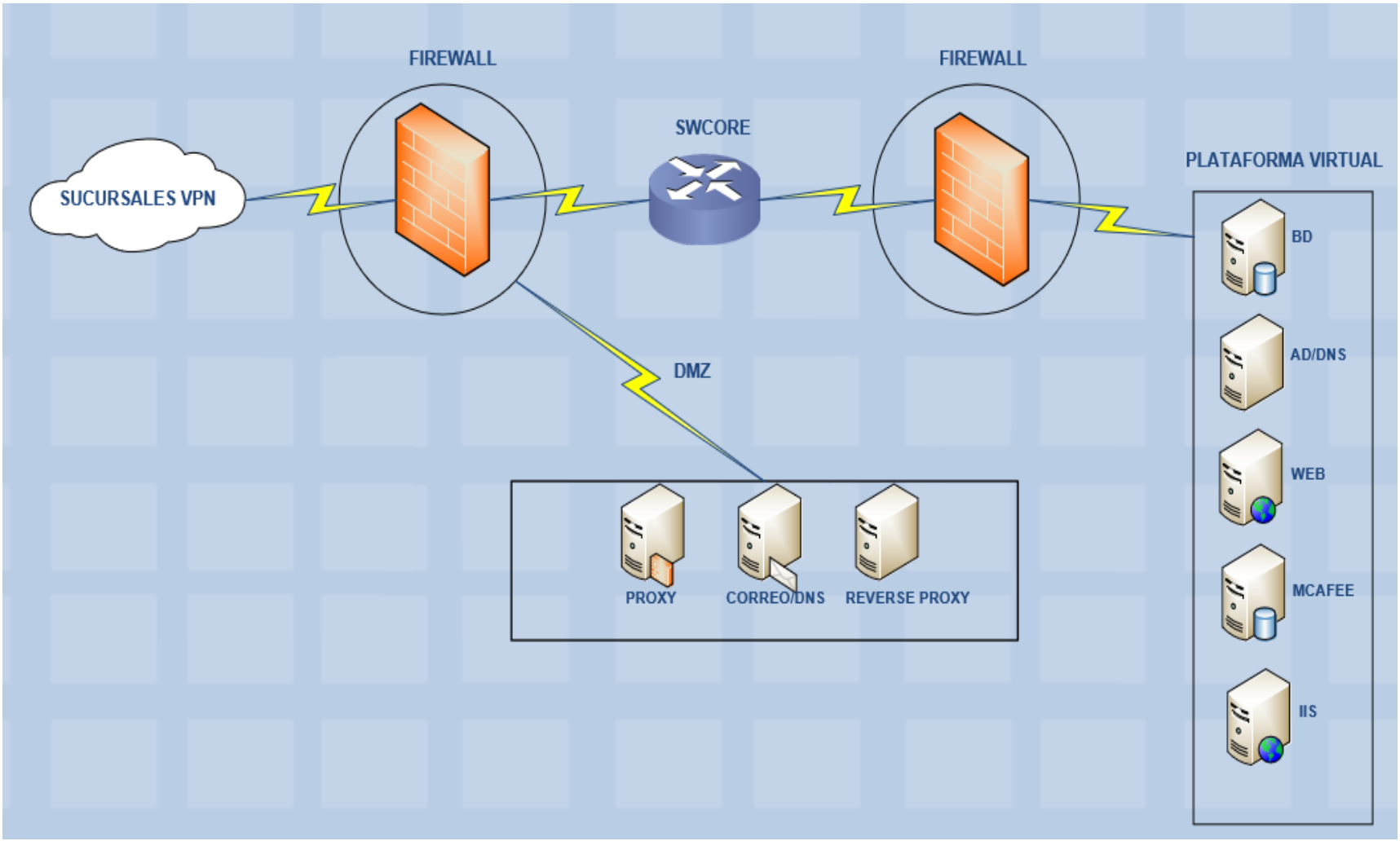
Fuente: (MAfee, 2018)

Figura 18. Diagrama de red actual



Fuente: (Elaboración propia)

Figura 19. Diagrama de red utilizado con MDE.



Fuente: (Elaboración propia)

6.3.1. Máquinas virtuales utilizadas para el demo

Para la presentación del demo de la solución de cifrado de McAfee Drive Encryption, se preparó un ambiente virtual, se utilizaron 2 servidores (Consola de Cifrado y AD) y 6 equipos clientes con las siguientes características:

Tabla 10. Máquina virtual 1.

Consola de Cifrado	Microsoft Windows Server 2012 R2 x64.
Características	Procesador: 2, 2.1Ghz. Memoria: 3.5GB. Disco Duro: 50GB
Servicios Instalados	Base de datos SQL Server Express 2012. Consola McAfee ePO 5.3.

Fuente: (Elaboración propia)

Tabla 11. Máquina virtual 2.

Directorio Activo	Microsoft Windows Server 2012 R2 x64.
Características	Procesador: 2, 2.1Ghz. Memoria: 3.5GB. Disco Duro: 50GB
Servicios Instalados	Creación y configuración de dominio ucn.edu.ni

Fuente: Elaboración propia.

Tabla 12. Máquina virtual 3.

UCN-LPT01	Microsoft Windows 8.1 x64.
Características	Procesador: 2, 2.1Ghz. Memoria: 2GB. Disco Duro: 30GB
Servicios Instalados	McAfee Agent 5.5.0.447 McAfee Drive Encryption Agent 7.2.4.2. McAfee Drive Encryption Go 7.2.4.2. McAfee Drive Encryption 7.2.4.2.

Fuente: Elaboración propia.

Tabla 13. Máquina virtual 4.

UCN-LPT02	Microsoft Windows 7 x64.
Características	Procesador: 2, 2.1Ghz. Memoria: 2GB. Disco Duro: 30GB
Servicios Instalados	McAfee Agent 5.5.0.447 McAfee Drive Encryption Agent 7.2.4.2. McAfee Drive Encryption Go 7.2.4.2. McAfee Drive Encryption 7.2.4.2.

Fuente: Elaboración propia.

Tabla 14. Máquina virtual 5.

UCN-LPT03	Microsoft Windows 10 x64.
Características	Procesador: 2, 2.1Ghz. Memoria: 2GB. Disco Duro: 50GB
Servicios Instalados	McAfee Agent 5.5.0.447 McAfee Drive Encryption Agent 7.2.6.6. McAfee Drive Encryption Go 7.2.6.6. McAfee Drive Encryption 7.2.6.6.

Fuente: Elaboración propia.

Tabla 15. Máquina virtual 6.

UCN-LPT04	Microsoft Windows 8.1 x64.
Características	Procesador: 2, 2.1Ghz. Memoria: 2GB. Disco Duro: 30GB
Servicios Instalados	McAfee Agent 5.5.0.447 McAfee Drive Encryption Agent 7.2.4.2. McAfee Drive Encryption Go 7.2.4.2. McAfee Drive Encryption 7.2.4.2.

Fuente: Elaboración propia.

Tabla 16. Máquina virtual 7.

UCN-LPT05	Microsoft Windows 8.1 x64.
Características	Procesador: 2, 2.1Ghz. Memoria: 2GB. Disco Duro: 30GB
Servicios Instalados	McAfee Agent 5.5.0.447 McAfee Drive Encryption Agent 7.2.4.2. McAfee Drive Encryption Go 7.2.4.2. McAfee Drive Encryption 7.2.4.2.

Fuente: Elaboración propia.

Tabla 17. Máquina virtual 8.

UCN-LPT06	Microsoft Windows 10 x64.
Características	Procesador: 2, 2.1Ghz. Memoria: 2GB. Disco Duro: 30GB
Servicios Instalados	McAfee Agent 5.5.0.447 McAfee Drive Encryption Agent 7.2.6.6. McAfee Drive Encryption Go 7.2.6.6. McAfee Drive Encryption 7.2.6.6.

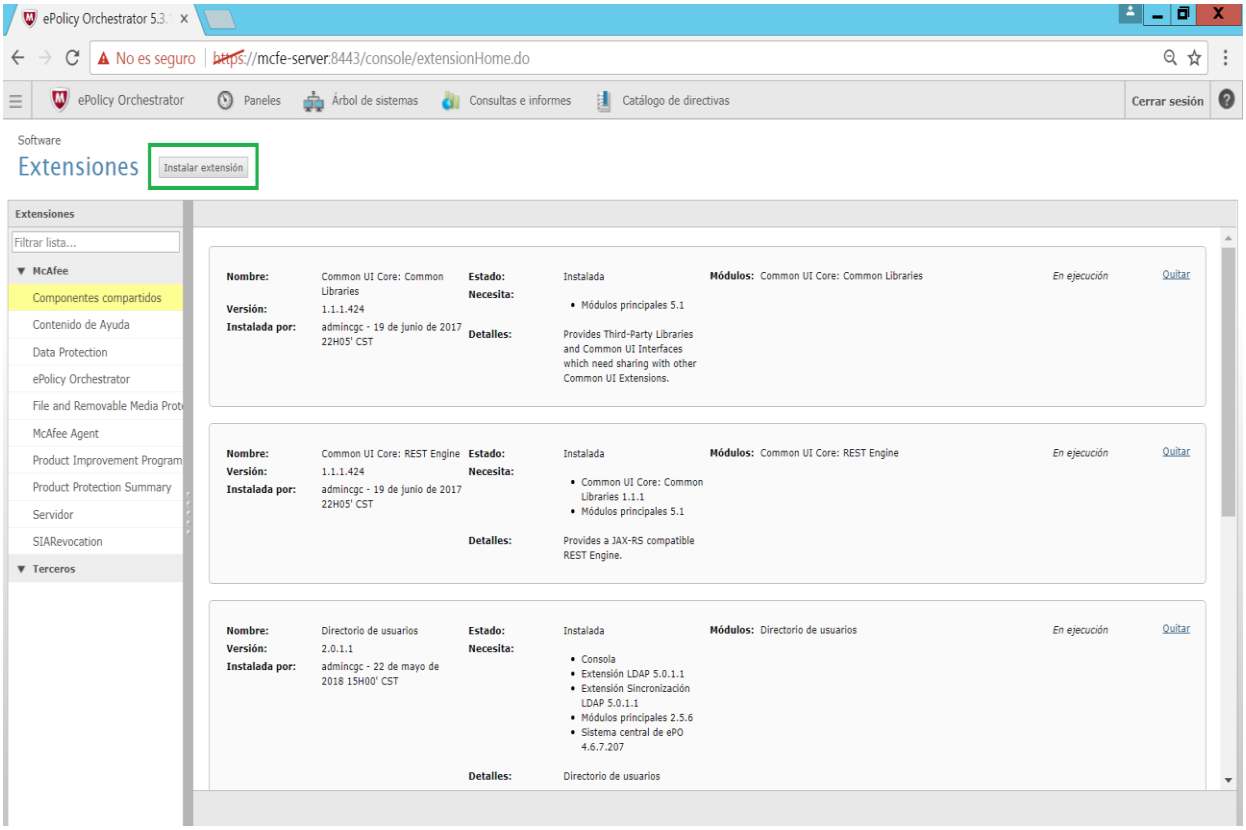
Fuente: Elaboración propia.

6.3.2. Instalaciones del lado del Servidor

Se instalan extensiones y paquetes de los productos de McAfee para el cifrado de los dispositivos portátiles.

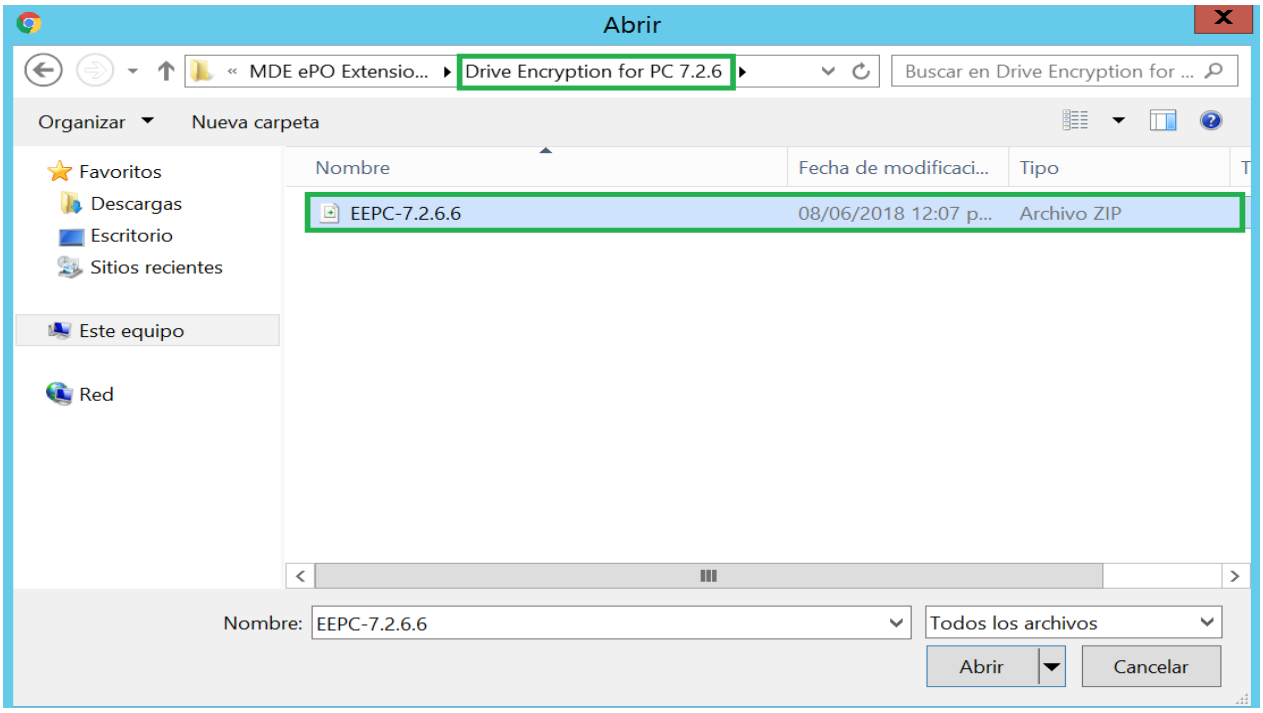
6.3.2.1. Extensiones y paquetes

Figura 19. Instalación de Extensiones.



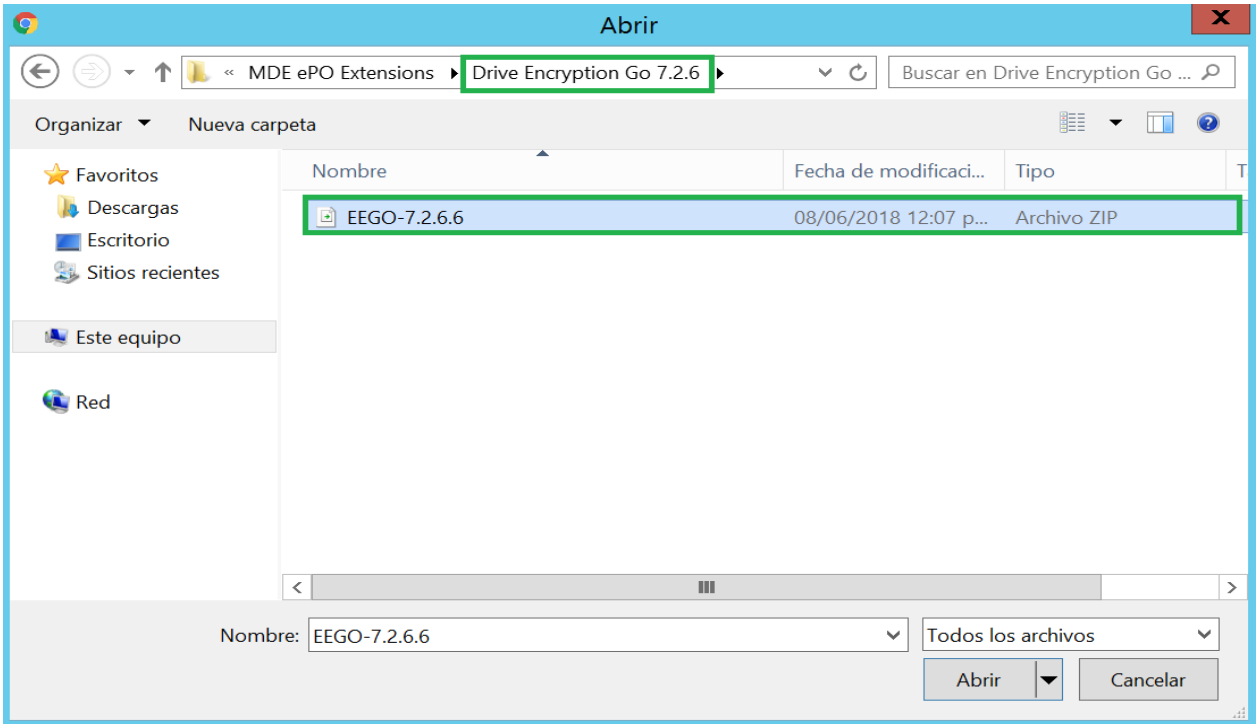
Fuente: (Elaboración propia)

Figura 20. Extension Drive Encryption for PC 7.2.6.6.



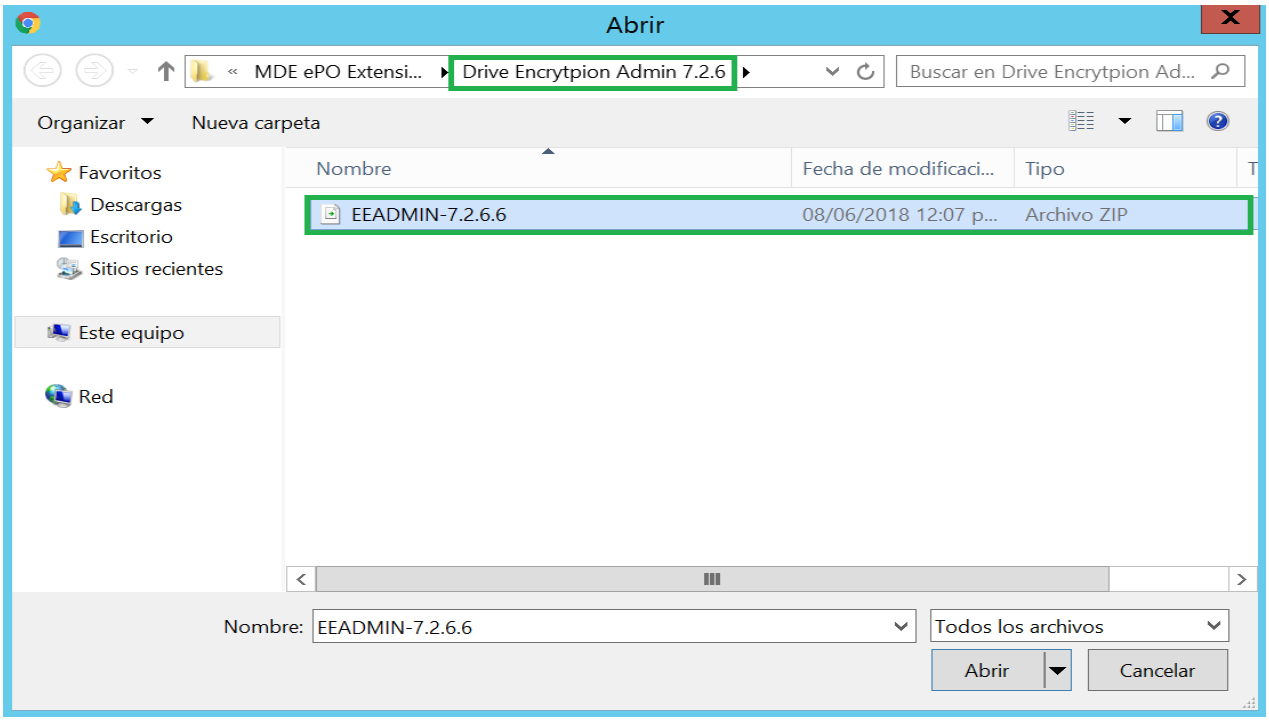
Fuente: (Elaboración propia)

Figura 21. Extension Drive Encryption Go 7.2.6.6.



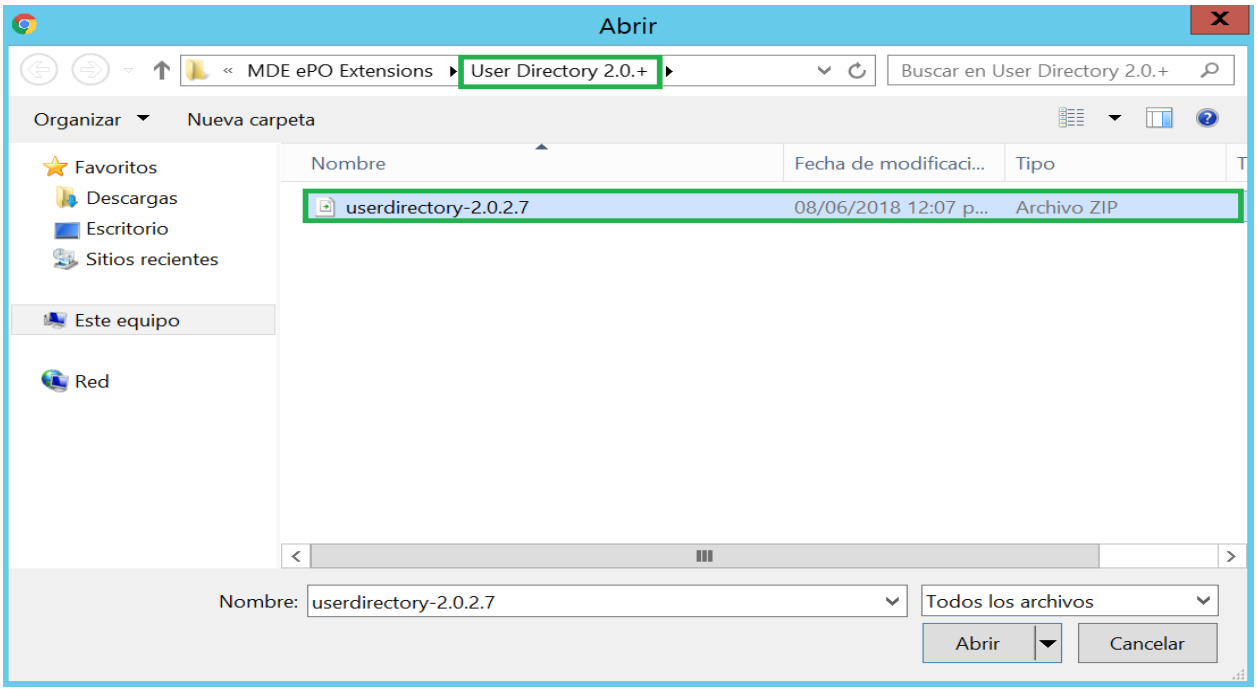
Fuente: (Elaboración propia)

Figura 22. Extension Drive Encryption Admin 7.2.6.6.



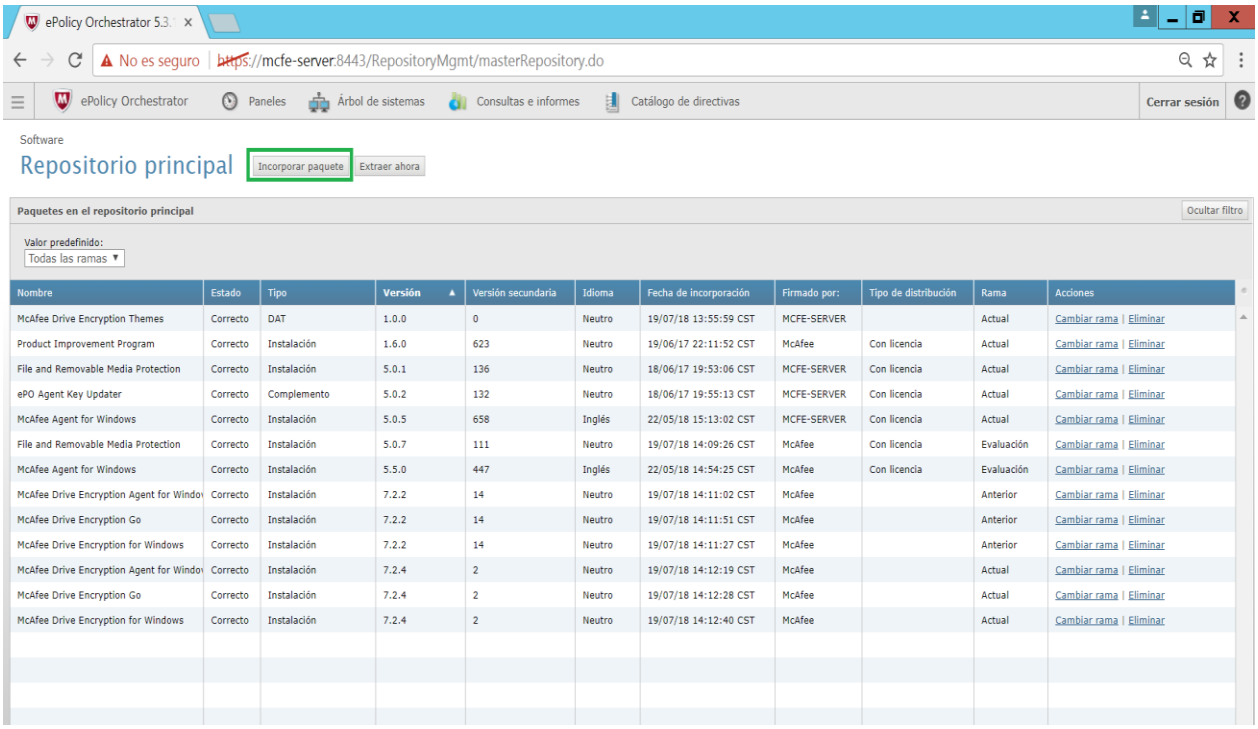
Fuente: (Elaboración propia)

Figura 23. Extension User Directory 2.0.2.7



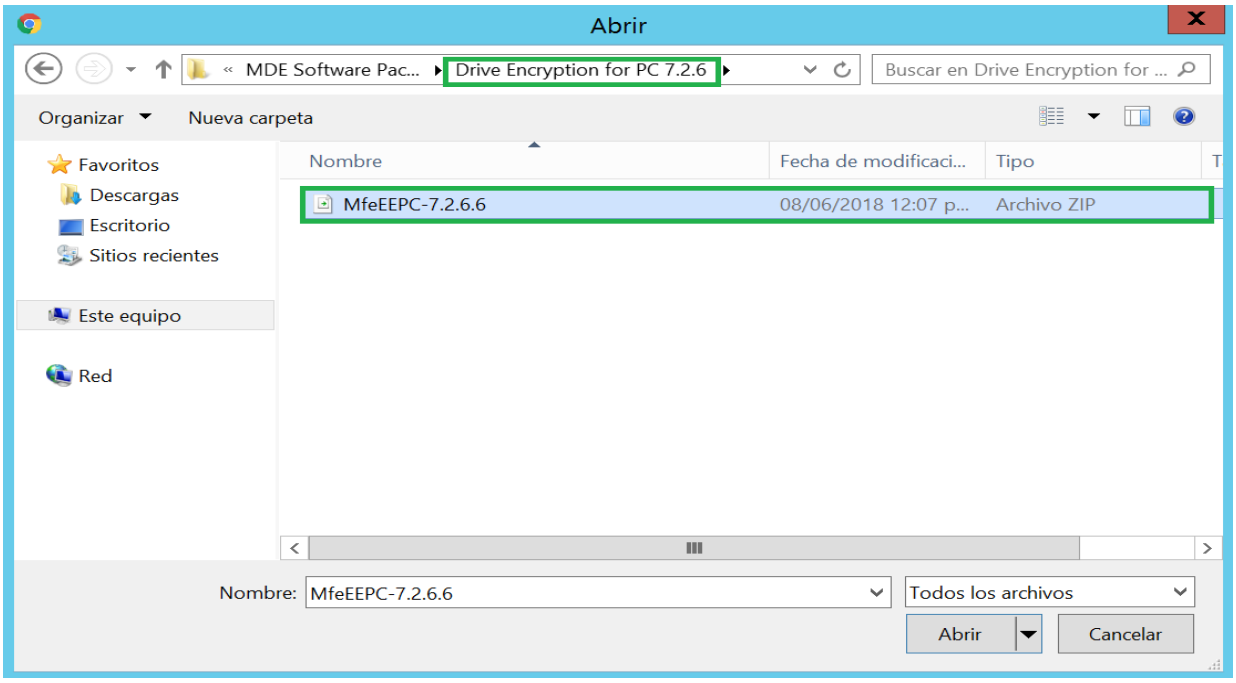
Fuente: (Elaboración propia)

Figura 24. Verificación de extensiones instaladas.



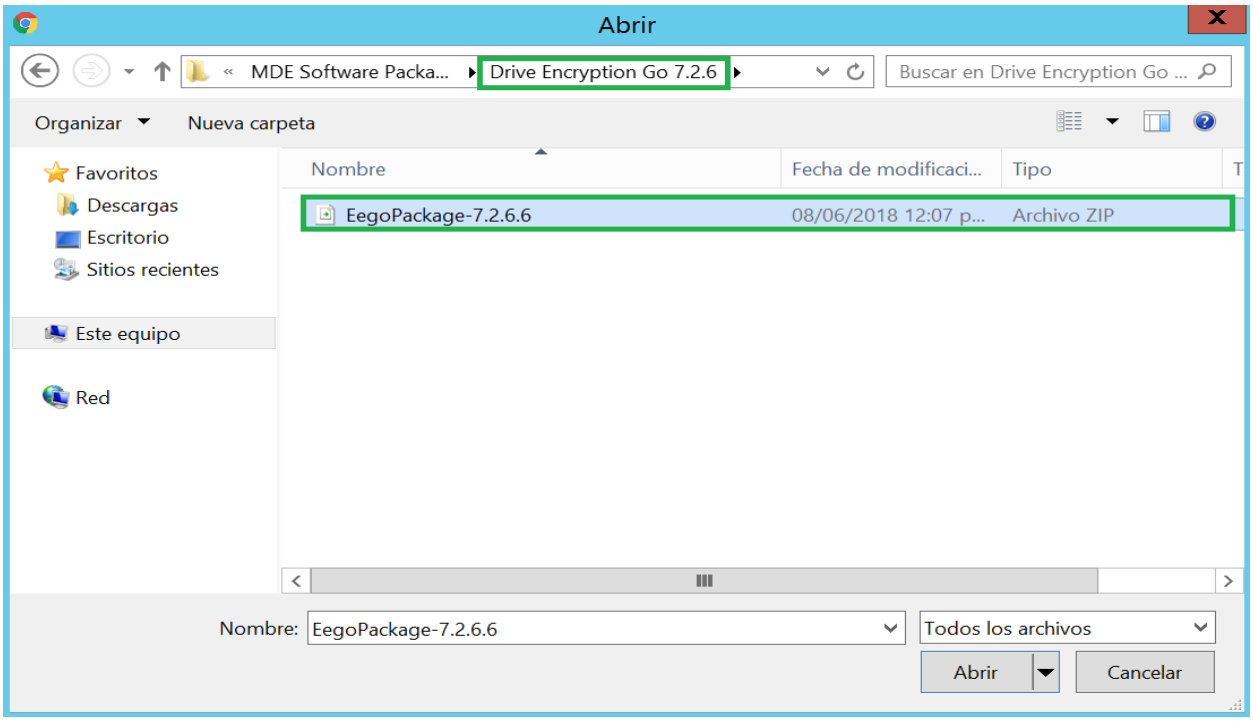
Fuente: (Elaboración propia)

Figura 25. Paquete Drive Encryption for PC 7.2.6.6.



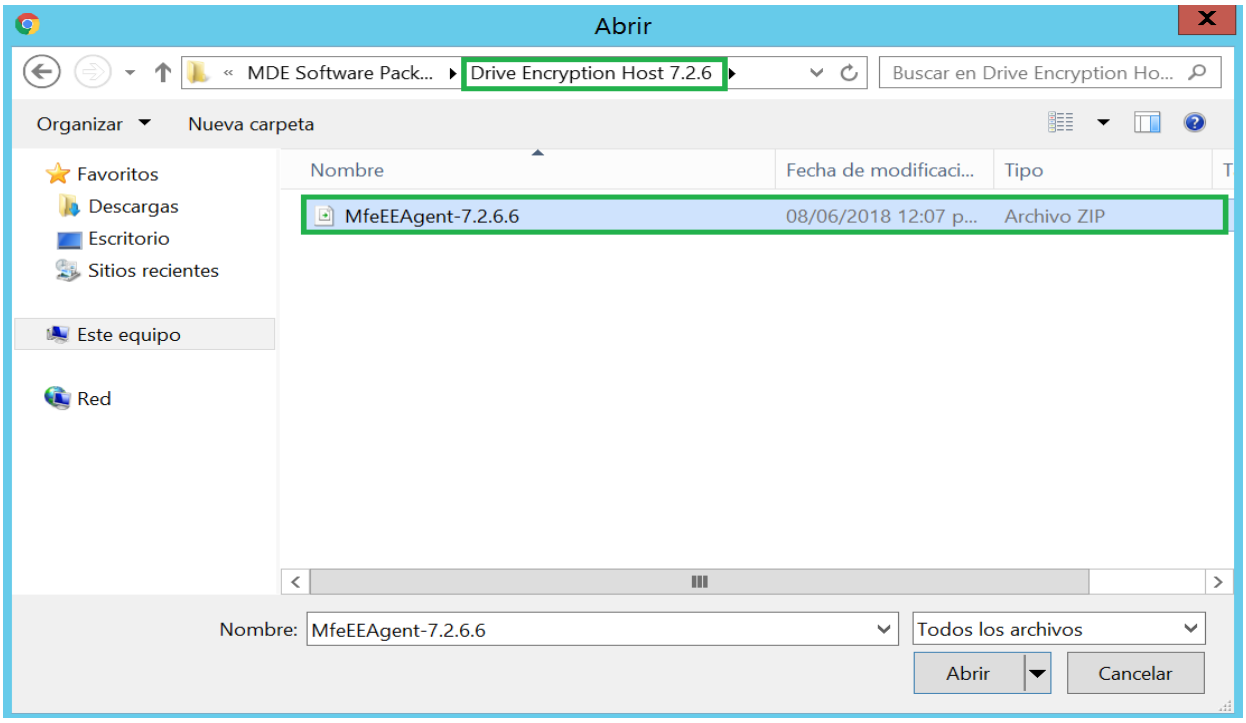
Fuente: (Elaboración propia)

Figura 26. Paquete Drive Encryption Go 7.2.6.6.



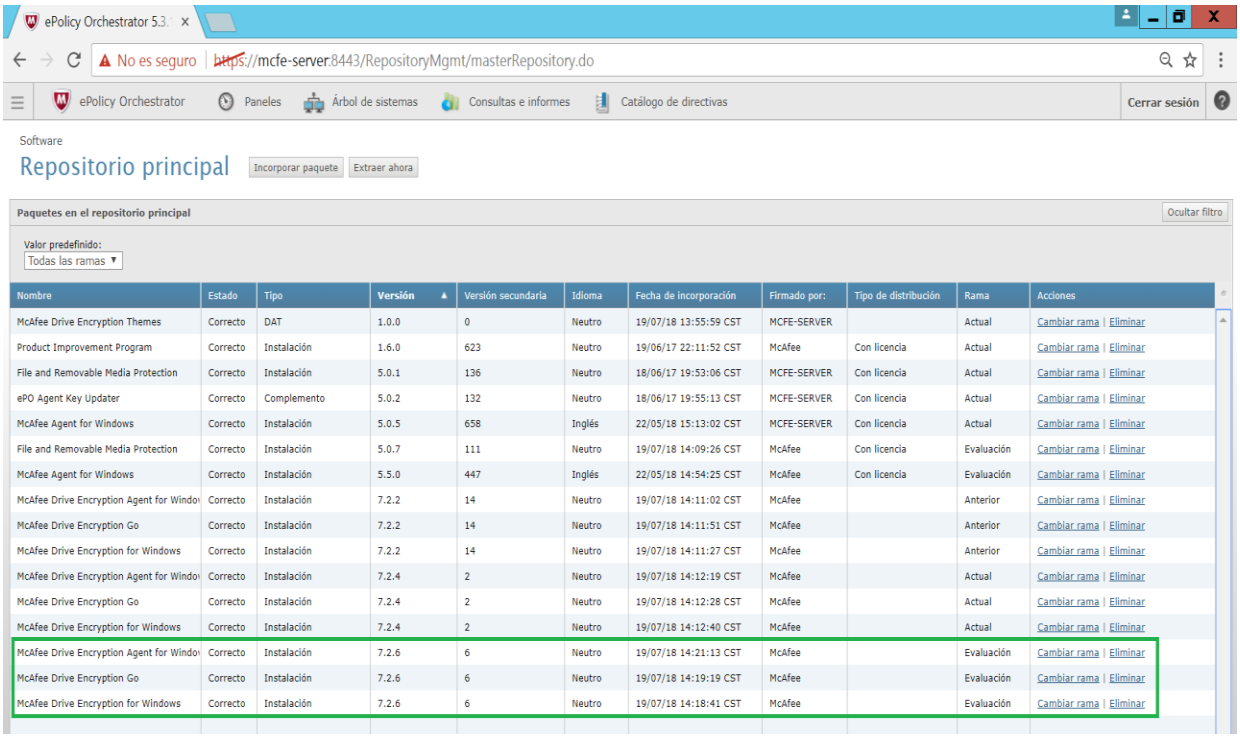
Fuente: (Elaboración propia)

Figura 27. Paquete Drive Encryption Host 7.2.6.6.



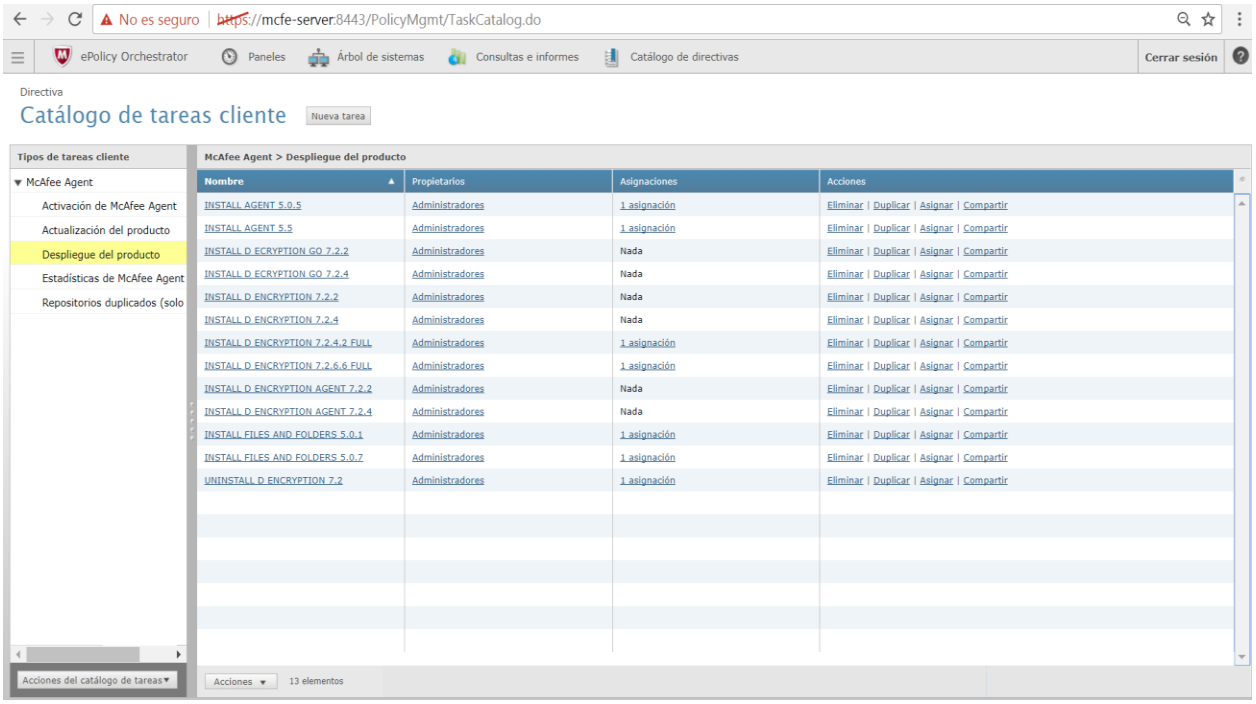
Fuente: (Elaboración propia)

Figura 28. Verificación de paquetes instalados.



Fuente: (Elaboración propia)

Figura 29. Catálogo de tareas clientes.



Fuente: (Elaboración propia)

6.3.3. Instalación a nivel de cliente.

De la solución McAfee ePolicy Orchertrator se utilizarán cuatro productos que son los siguientes:

1. **McAfee Agent 5.5.0.447:** es el componente del lado del cliente que posibilita la comunicación segura entre McAfee ePolicy Orchestrator (McAfee ePO) y los productos gestionados. También sirve como actualizador para productos gestionados y no gestionados de McAfee.McAfee ePO solo puede gestionar los sistemas si tienen un agente instalado.
2. **McAfee Drive Encryption Agent 7.2.4.2:** Es el componente del lado del cliente para realizar la sincronización con el servidor McAfee ePO, obtiene todos los usuarios asignados.
3. **McAfee Drive Encryption Go 7.2.4.2:** Es una utilidad que nos indica la disposición del sistema para instalar DE. Proporciona algunas pruebas iniciales del sistema para verificar que estará listo para instalar y activar el producto.
4. **McAfee Drive Encryption 7.2.4.2:** también llamado cifrado total de disco, es un software de cifrado que ayuda a proteger los datos de las tablets, portátiles y PCs con Microsoft Windows instalado para impedir la fuga de datos confidenciales, en particular en caso de pérdida o robo. Está diseñado para que todos los datos del disco de los sistemas sean ininteligibles para las personas no autorizadas, lo que a su vez ayuda a cumplir los requisitos de las normativas.

Para realizar el proceso de instalación de los productos de McAfee en las computadoras laptops en la Universidad Central de Nicaragua, es necesario seguir los siguientes pasos:

1. Actualizar la versión del BIOS a la última versión estable.
2. Realizar un respaldo FULL de toda la información del disco duro de la laptop que será cifrada por la solución McAfee.

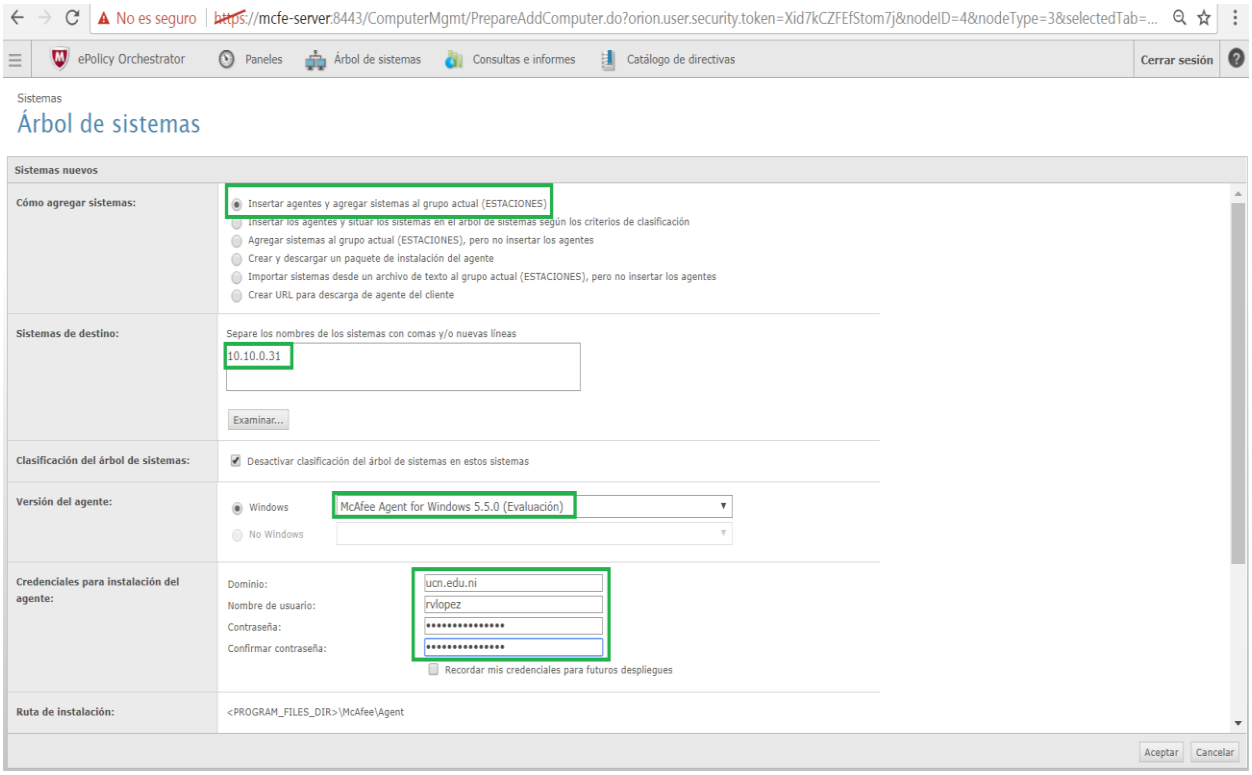
   Tiempo Estimado: 3 Horas.
3. Encender la laptop y conectarla a un punto de red.

   Tiempo Estimado: 5 Minutos.
4. Verificar que no tenga instalado ningún programa utilizado para cifrar la información. En el caso de tenerlo instalado, se deberá a proceder a desinstalarlos para iniciar la instalación de los paquetes de McAfee.

   Tiempo Estimado: 30 Minutos.
5. Desde la consola Epo instalar el agente de McAfee.

   Tiempo Estimado: 10 Minutos.

Figura 30. Instalación de Agente



Fuente: (Elaboración propia)

6. Una vez realizado el paso anterior, se deberá de reiniciar la laptop.

   Tiempo Estimado: 10 Minutos.

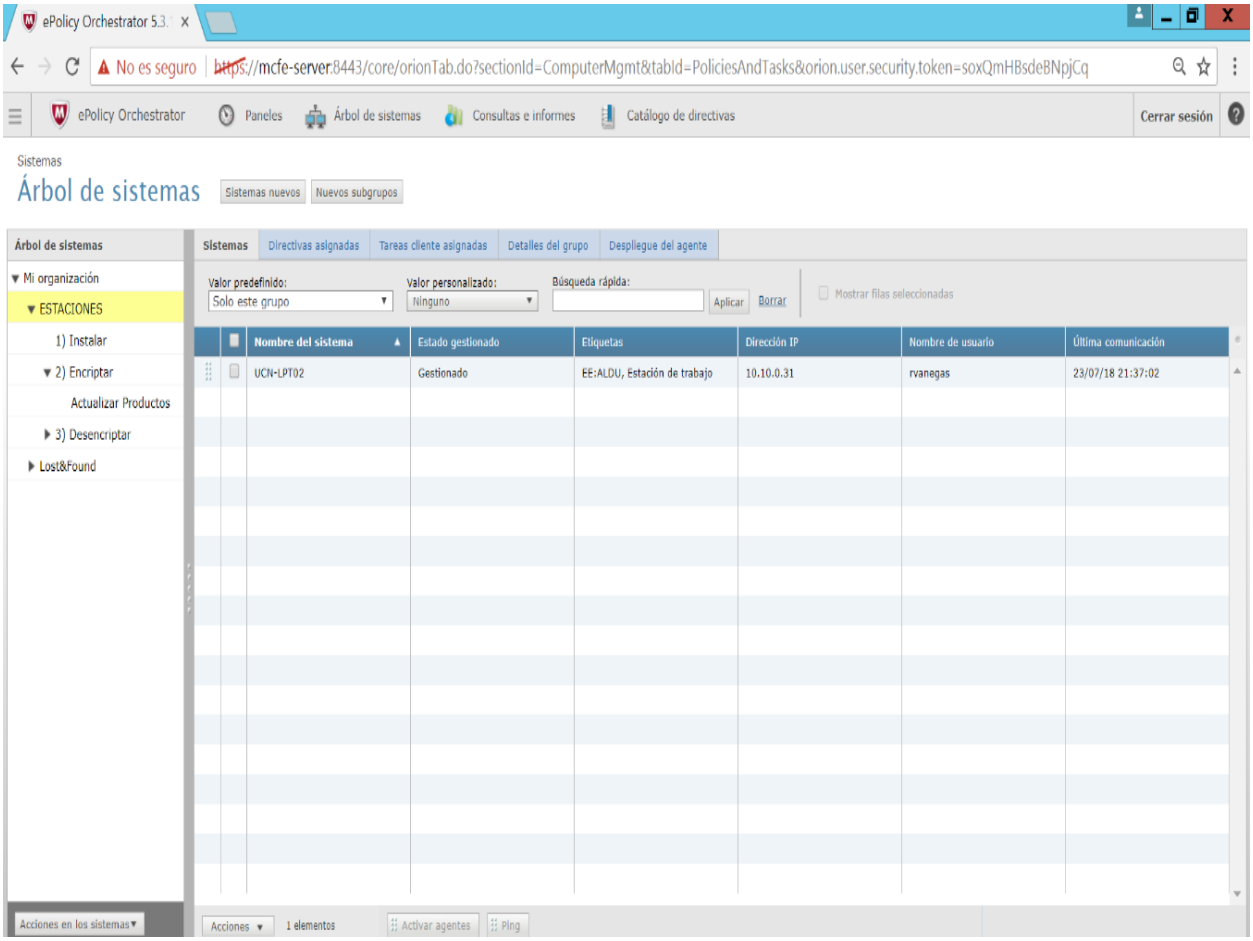
7. Iniciar sesión en la laptop para continuar.

   Tiempo Estimado: 5 Minutos.

8. Verificar en el servidor de consola Epo McAfee que el equipo UCN-LPT02 aparezca en la carpeta "**ESTACIONES"** y en estado **"Gestionado".**

   Tiempo Estimado: 5 Minutos.

Figura 31. Verificación de equipo.



Fuente: (Elaboración propia)

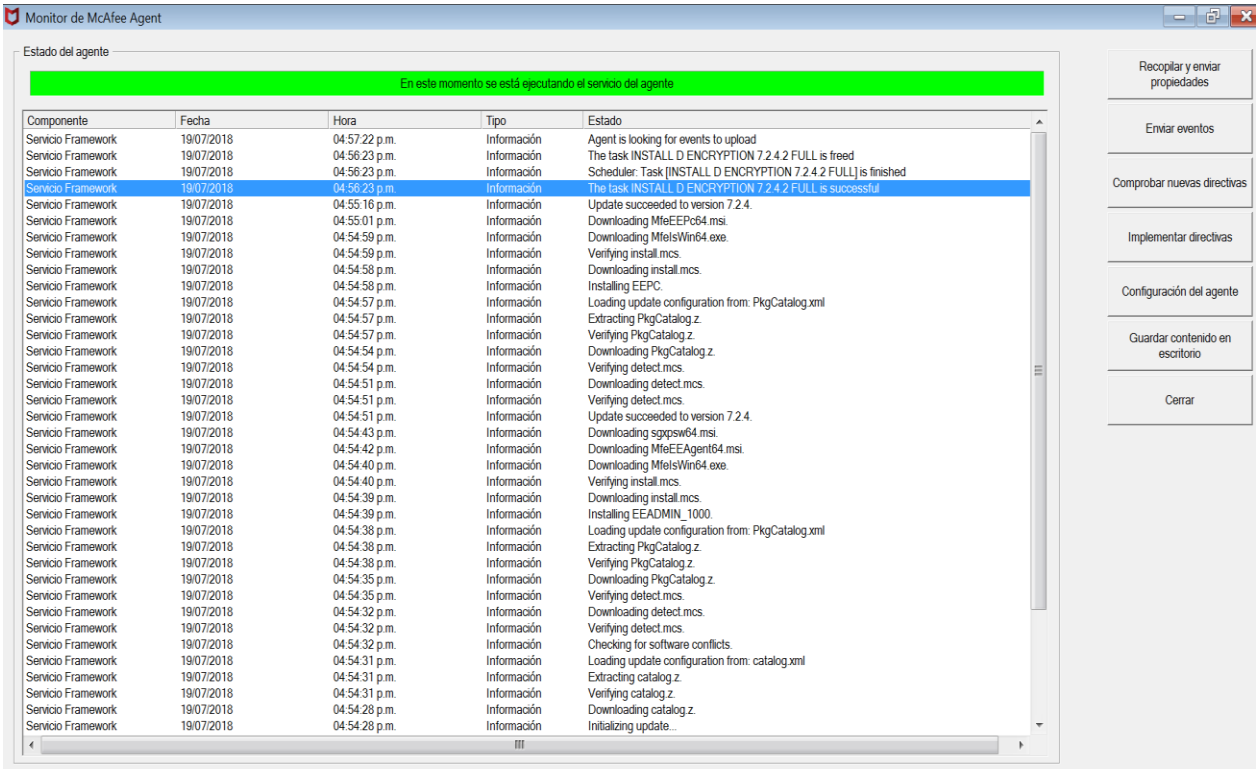
9. Mover la laptop a carpeta **“Instalar”**.

Tiempo Estimado: 15 Minutos.

En este paso se instalan automáticamente los siguientes paquetes en el siguiente orden:

8.1. McAfee Drive Encryption Agent 7.2.4.2
8.2. McAfee Drive Encryption Go 7.2.4.2
8.3. McAfee Drive Encryption 7.2.4.2

Figura 32. Instalación de paquetes.



Fuente: (Elaboración propia)

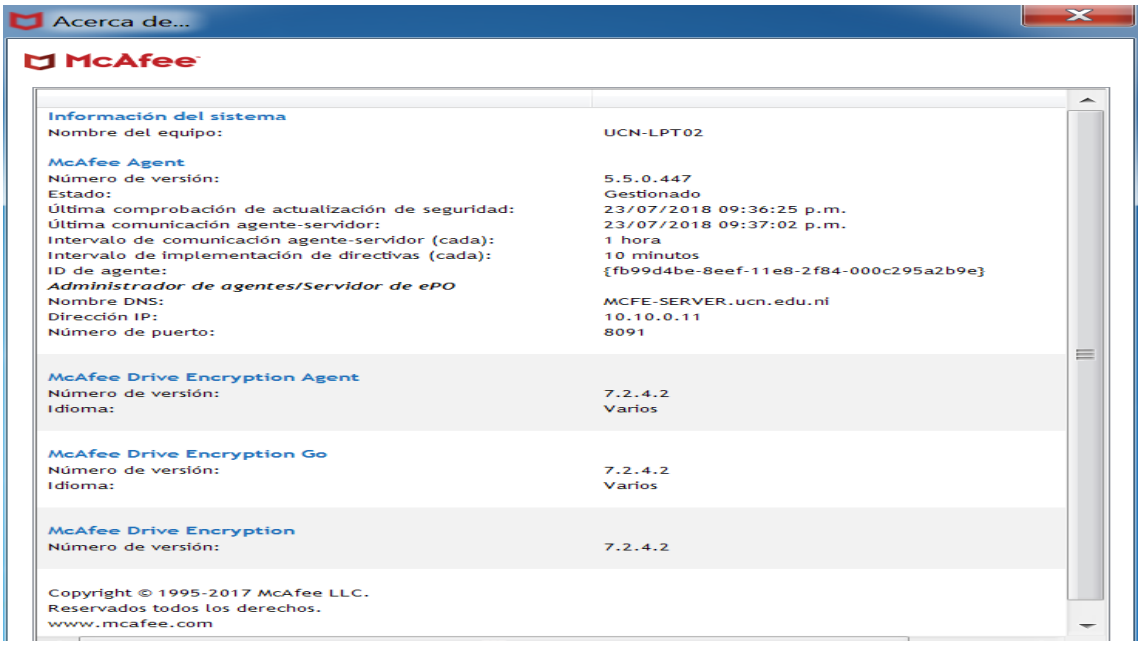
10. Una vez que los productos fueron instalados, el equipo enviará un mensaje de reinicio.

11. La verificación de los paquetes en el equipo UCN-LPT02 se puede hacer desde la consola EPO del servidor McAfee (**“Árbol de Sistemas”**) o desde el equipo. **Tiempo Estimado: 5 Minutos**.

Figura 33. Verificación de paquetes instalados.

Fuente: (Elaboración propia)

Figura 34. Verificación de paquetes instalados.

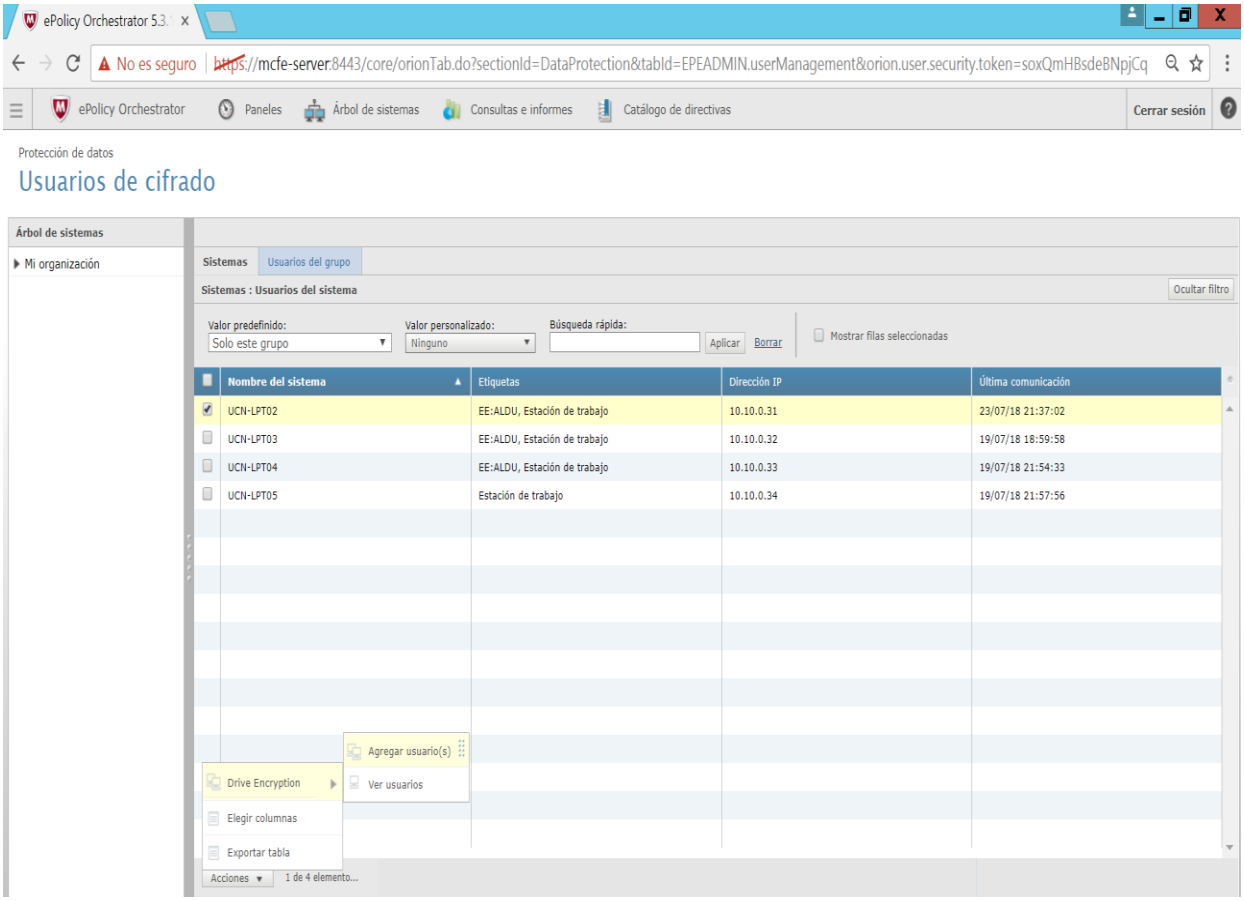


Fuente: (Elaboración propia)

12. Agregar los usuarios autorizados a ingresar a la laptop.

Tiempo Estimado: 5 Minutos. Esto se realiza en la opción **“Usuarios de cifrado”.**

Figura 35. Agregar usuarios en equipo.

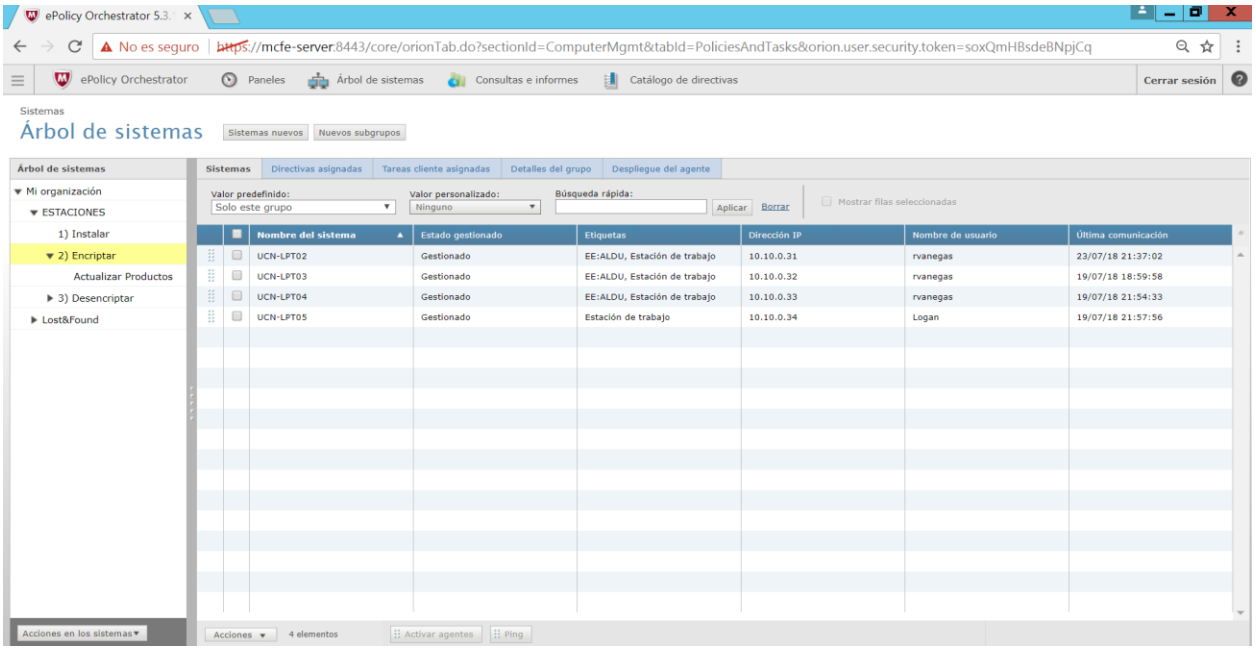


Fuente: (Elaboración propia)

13. Mover el equipo a la carpeta **“Encriptar”** desde la opción árbol de sistemas.

Tiempo Estimado: 5 Minutos.

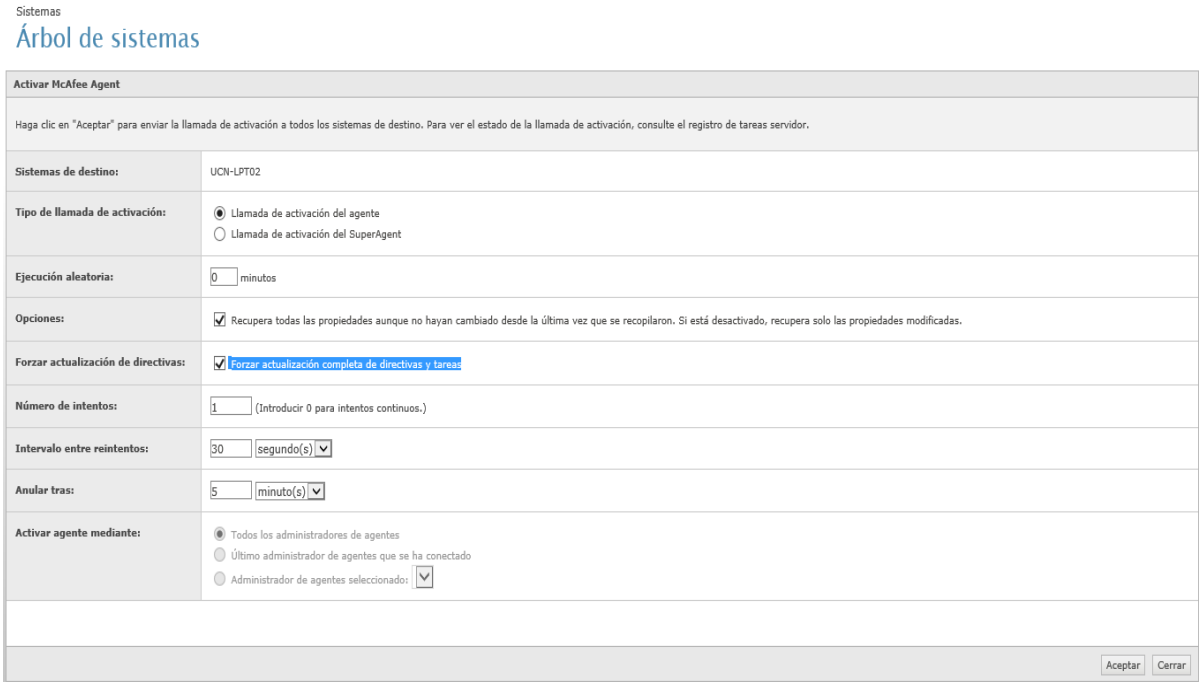
Figura 36. Mover equipo a Encriptar.



Fuente: (Elaboración propia)

14. Forzar las políticas desde la consola EPO McAfee para iniciar el proceso de encriptación de todo el disco duro.

Figura 37. Forzar políticas a equipo.



Fuente: (Elaboración propia)

15. Después de unos minutos de validación, inicia el cifrado en el equipo UCN-LPT02. Este proceso es bastante tardado porque lee todos los sectores del disco, este tiempo puede variar, va en dependencia de los recursos del equipo y de la capacidad del disco.

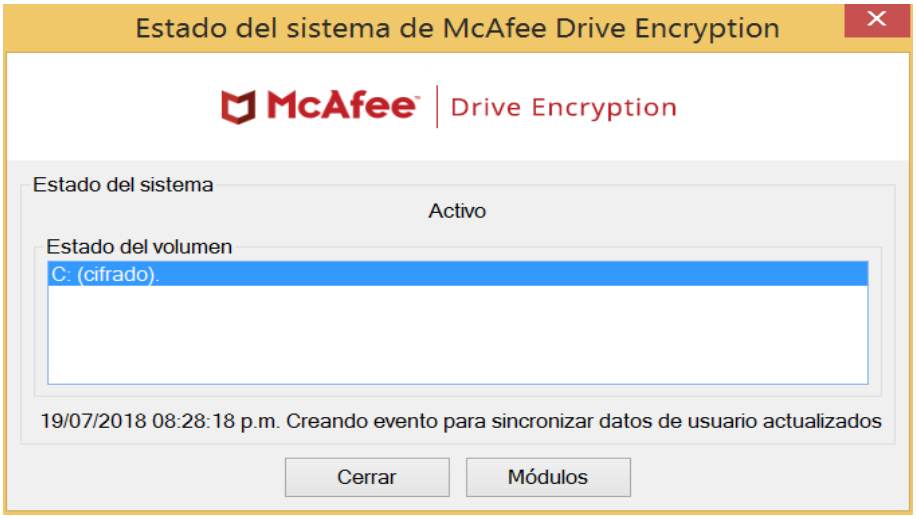
    Tiempo Estimado: De 5 a 8 Horas.

Figura 38. Inicio de cifrado en equipo.

Fuente: (Elaboración propia)

16. El proceso de cifrado se ha realizado satisfactoriamente en el equipo UCN-LPT02.

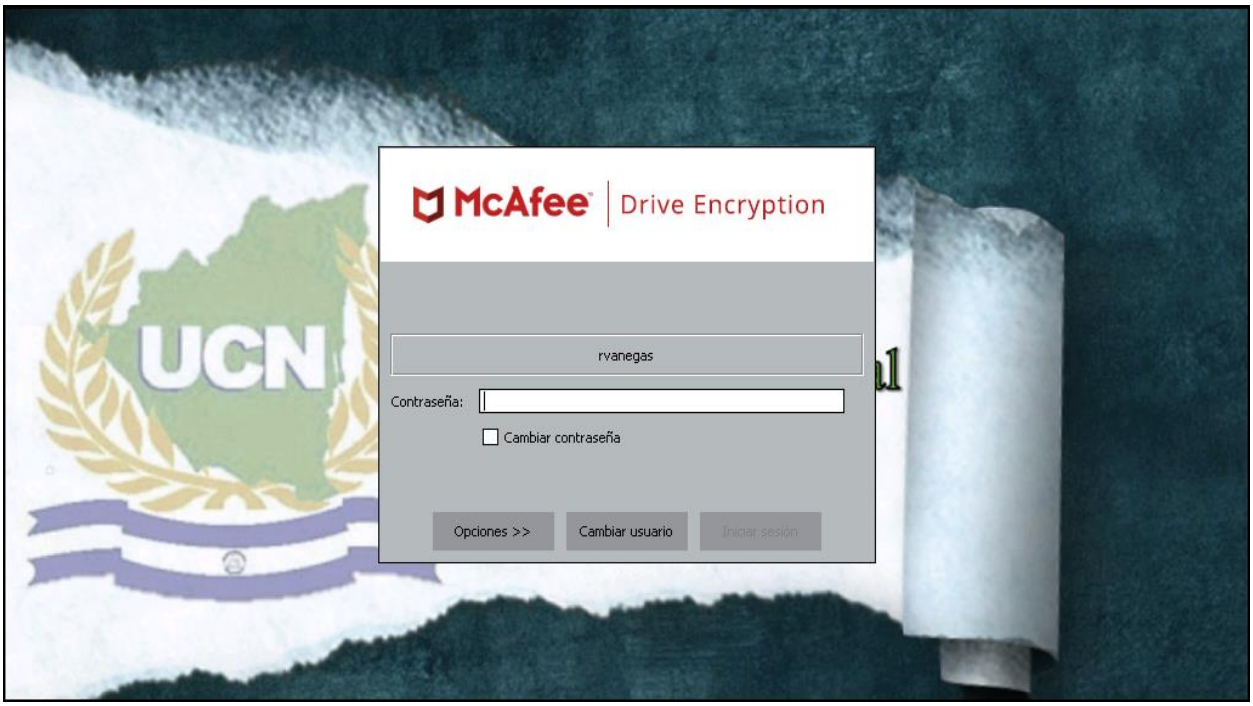
Figura 39. Equipo cifrado.



Fuente: (Elaboración propia)

17. Una vez que se hayan instalados los paquetes y la laptop sea reiniciada, aparecerá la pantalla de McAfee solicitando usuario y contraseña de acceso.

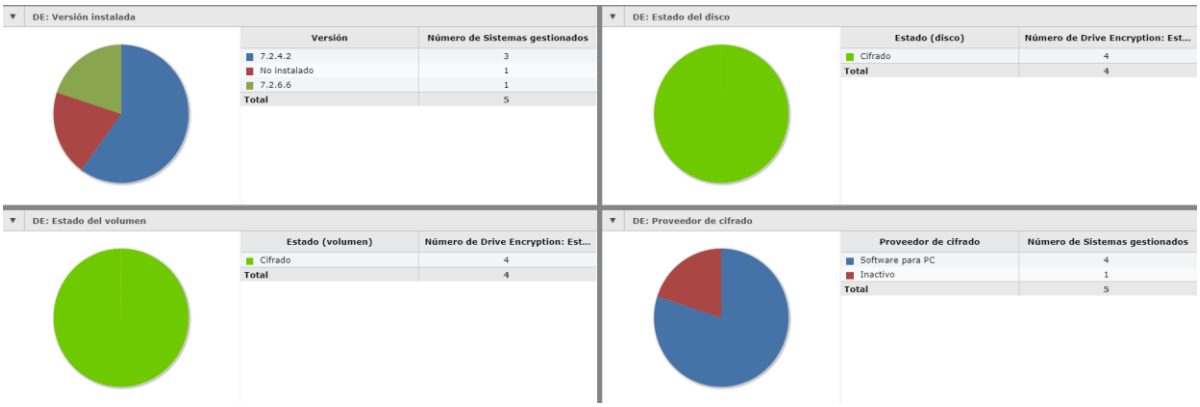
Figura 40. Inicio de sesión de cifrado.



Fuente: (Elaboración propia)

Nota: La contraseña por defecto se define en la consola Epo, una vez digitada el sistema le solicitará cambio de contraseña. Esta clave puede ser diferente a la que utiliza en el Active Directory pero una vez que ingresa al sistema operativo se actualizarán las políticas y la contraseña será sincronizada con el Active Directory y esta será la clave a utilizar. Esta sincronización se realizará cada 5 minutos de forma automática y transparente al usuario.

Figura 41. Detalle dispositivos portátiles cifrados.



Fuente: (Elaboración propia)

Figura 42. Dispositivos portátiles cifrados.

DE: Estado del disco -> Cifrado

Valor personalizado: Ninguno

Mostrar filas seleccionadas

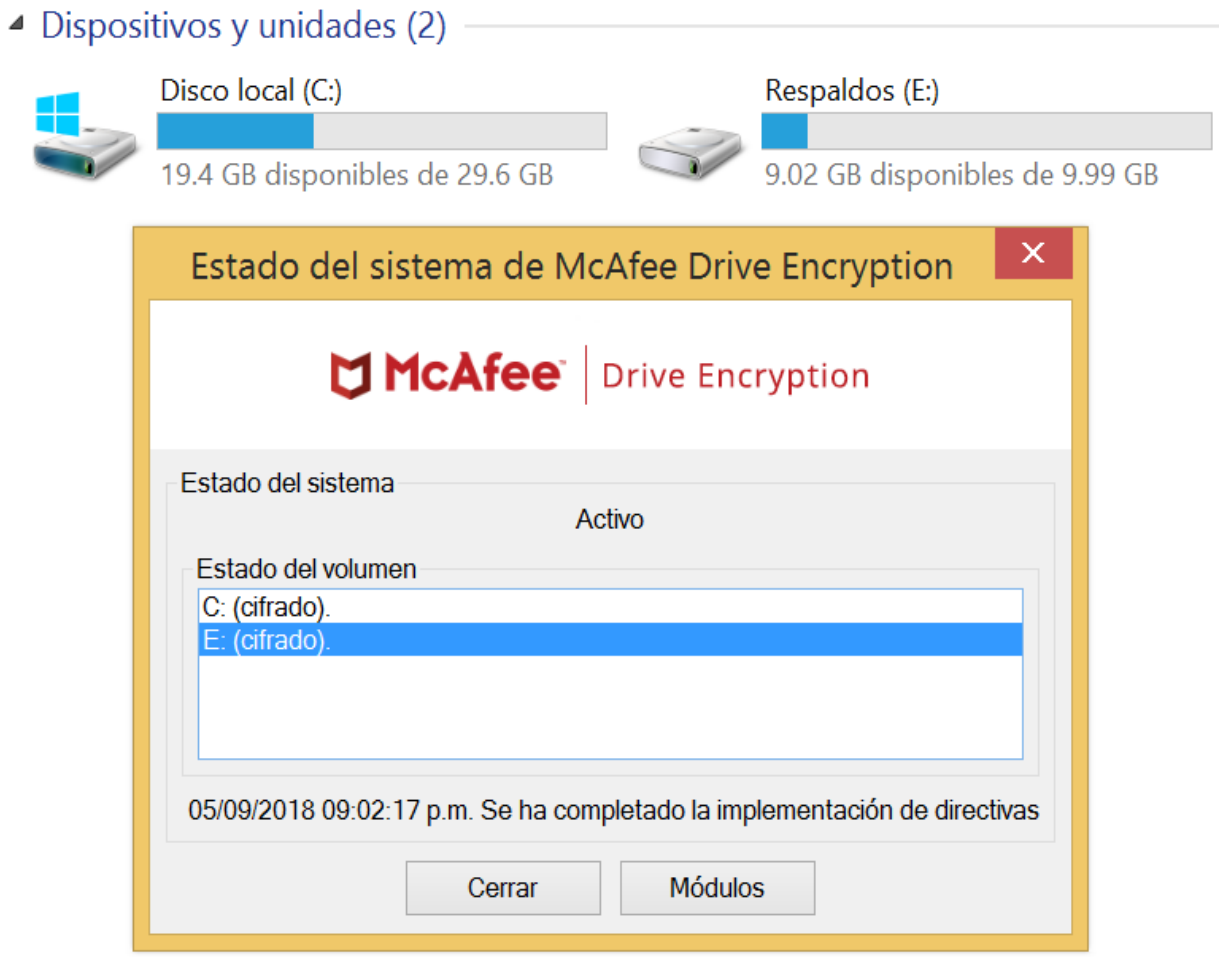
Nombre del sistema	Número de modelo	Número de serie	Estado (disco)	Tamaño (MB)
UCN-LPT02	VMware Virtual S		Cifrado	30.720
UCN-LPT03	VMware Virtual S		Cifrado	51.200
UCN-LPT04	VMware Virtual S		Cifrado	30.720
UCN-LPT05	VMware Virtual S		Cifrado	30.720

Fuente: (Elaboración propia)

6.4. Pruebas realizadas

Se verificó que los discos C y D se encontraran cifrados en el equipo portátil UCN-LPT02, desde el sistema operativo como se puede observar en la figura 43, se tiene acceso a la información contenida en los discos duros.

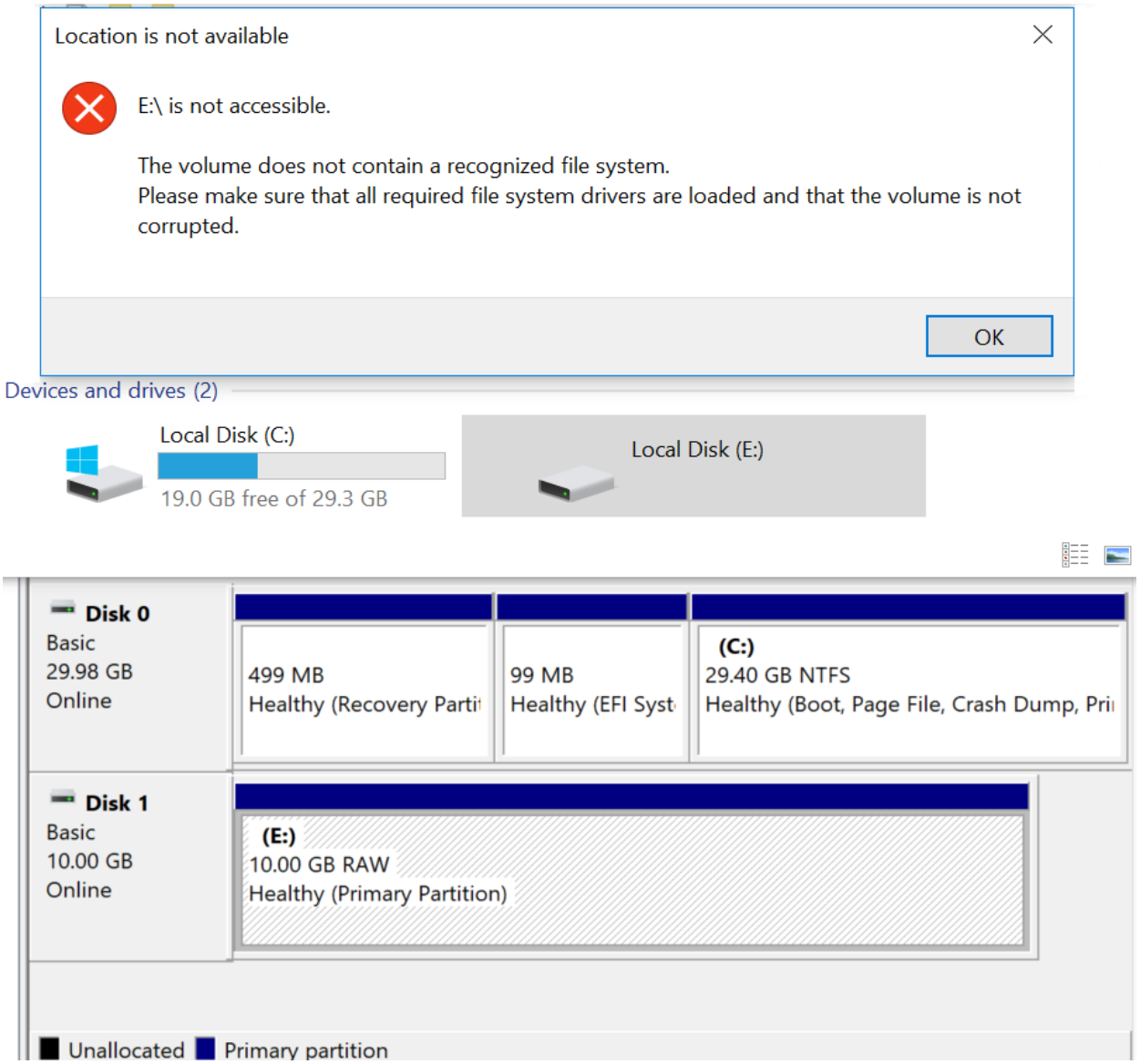
Figura 43. Discos duros cifrados.



Fuente: (Elaboración propia)

Si retiramos el disco “E” y lo conectamos por medio de un enclosure al equipo UCN-LPT06, la información no se logra visualizar, aunque el sistema operativo lo reconozca y le asigne una unidad, esto se sucede porque el disco se encuentra cifrado como se puede apreciar en la figura 44.

Figura 44. Disco no accesible



Fuente: (Elaboración propia)

7. Conclusiones

La seguridad de la información, es un activo muy valioso para una organización, se requiere de mucho esfuerzo por parte del personal y una inversión inicial por parte de la organización, para implementar diferentes soluciones para protegerla de personal no autorizado.

Durante esta investigación por medio de entrevistas, pruebas, análisis de aplicaciones de cifrado, revisión de los dispositivos portátiles en la Universidad Central de Nicaragua se llegaron a las siguientes conclusiones:

- Producto del análisis de la situación actual en la Universidad, se encontró que no existe ningún mecanismo de protección de la información en los dispositivos portátiles, la información está expuesta y puede ser accedida muy fácilmente en caso de pérdida o robo del dispositivo portátil. Se demostró en las pruebas iniciales, que la información puede ser accedida por personal no autorizado, no se necesitan muchos conocimientos técnicos para acceder a la información contenida en los discos duros.

- Se evaluaron diferentes soluciones de seguridad para la protección de la información en los dispositivos portátiles, tomando como referencia el cuadrante mágico de Gartner y analizando las características de cada una de ellas, con el objetivo de seleccionar la aplicación más óptima para las convecciones de la UCN. A través de un demo de la solución McAfee Drive Encryption, se pudo corroborar que solo personal autorizado puede ingresar a los dispositivos portátiles.

- Se diseñó la infraestructura de seguridad necesaria para la implementación del sistema de protección, se tomó como referencia el diseño de la infraestructura existente en la Universidad. Una vez cifrado el disco duro con la solución implementada en el demo, no se puede tener acceso a los datos aun retirándolo y conectándolo a través de un enclosure en otro equipo. En caso de olvido de la contraseña de un usuario permitido, a través de un procedimiento de la solución es posible acceder al dispositivo portátil, siempre y cuando se tenga acceso al servidor de consola. Se pueden recuperar los datos cifrado en caso de daño completo del equipo con disco duro en buen estado o que el sistema operativo se corrompa, esto se realiza a través de un procedimiento contenido en el anexo de este documento.

8. Recomendaciones

Una vez finalizada la investigación, se recomiendan las siguientes acciones a tomar en cuenta en la UCN:

- Del inventario de equipos portátiles, se debe de revisar que equipos se deben priorizar para la protección de la información.

- Capacitación continua al personal encargado de administrar este sistema, con el objetivo de dar solución a los problemas presentados y únicamente requerir del soporte cuando sea meramente necesario.

- Mantener los productos actualizados al menos 2 veces al año de la solución McAfee Drive Encryption en los equipos portátiles, esta práctica nos garantiza una mejor funcionalidad en los equipos portátiles.

- Mantener actualizado la documentación técnica de la solución McAfee Drive Encryption.

- Garantizar el soporte técnico de la solución, para lograr una asistencia remota o en sitio cuando la situación lo requiera.

- Evaluar los otros productos que incluye el paquete de licencia de McAfee para la implementación de acuerdo a las necesidades de la UCN.

9. Bibliografía

- Gordon, (2018). No todo está perdido si te roban la computadora. [en linea] Recuperado de: https://www.nytimes.com/es/2018/03/19/computadora-encriptacion-robo/ [consultado 25 de julio 2018].

- Eset, (2013). A más del 58% de los usuarios en Latinoamérica le han robado su teléfono móvil. [en linea] Recuperado de: https://www.welivesecurity.com/la-es/2013/02/06/mas-58-usuarios-latinoamerica-han-robado-telefono-movil/ [consultado 15 de diciembre 2017].

- jaimemontoya, M. (2017). Estándar Internacional ISO/IEC 27002 (página 2) - Monografias.com. [en línea] Monografias.com. Recuperado de: http://www.monografias.com/trabajos67/estandar-internacional/estandar-internacional2.shtml [consultado 25 de febrero 2018].

- Iso27000.es. (2013). ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información. [en línea] Recuperado de: http://www.iso27000.es/sgsi.html [Consultado 25 de marzo 2018].

- Eset-la. (2014). Cifrado de la información. [en linea] Recuperado de: https://www.welivesecurity.com/wp-content/uploads/2014/02/guia_cifrado_corporativo_2014v2.pdf [Consultado 30 de marzo 2018].

- Roa, J.F. (2013). “Seguridad Informática”. España: McGraw-Hill.

- Gartner. (2018). Magic Quadrant for Endpoint Protection Platforms. [en línea] Recuperado de: https://www.gartner.com/doc/reprints?id=1-4PGZC8P&ct=180126&st=sb&submissionGuid=a2b7821a-0ce0-4f53-8fa6-cda20d4c492c [Consultado 02 de marzo 2018].

- McAfee. McAfee Drive Encryption 7.1.0 Revision B (2015). Recuperado de: https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/24000/PD24867/en_US/de_710_product_guide_en_us_RevB.pdf [Consultado 25 de julio 2018].

- McAfee ePolicy Orchestrator 5.9.0 (2017). Recuperado de https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/26000/PD26915/en_US/epo_590_ig_0b00_en-us.pdf [Consultado 30 de diciembre 2017].

- McAfee Drive Encryption 7.2.5 Installation Guide (2018). Recuperado de https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/27000/PD27691/en_US/mde_725_ig_en-us.pdf [Consultado 15 de junio 2018].

- Management of Native Encryption (2016). Recuperado de: https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-management-of-native-encryption.pdf [Consultado 15 de julio 2018].

- Puertos que requiere ePolicy Orchestrator para la comunicación a través de firewall (2018). Recuperado de https://kc.mcafee.com/corporate/index?page=content&id=KB66797&locale=es_ES&viewlocale=es_ES [Consultado 30 de abril 2018].

- Ayuda del administrador de SafeGuard Enterprise. (2017). Recuperado de https://docs.sophos.com/esg/sgn/8-0/admin/win/en-us/webhelp/index.htm#concepts/SafeGuard_FullDiskEncryption.htm [Consultado 15 de enero 2018].

- Safeguard Encryption. (2017). Recuperado de https://www.sophos.com/es-es/products/safeguard-encryption.aspx [Consultado 15 de enero 2018].

- Released by IDRIX (2018). VeraCrypt User's Guide, version 1.23. Recuperado de https://www.veracrypt.fr/en/Home.html [Consultado 20 de septiembre 2018].

- Released by IDRIX (2018). System Encryption. Recuperado de https://www.veracrypt.fr/en/System%20Encryption.html [Consultado 10 de abril 2018].

- BitLocker (2015). Recuperado de https://technet.microsoft.com/es-es/library/mt404680(v=vs.85).aspx [Consultado 30 de marzo 2018].

- Novedades en BitLocker (2015). Recuperado de https://technet.microsoft.com/es-es/library/mt404680(v=vs.85).aspx [Consultado 30 de marzo 2018].

10. Anexos

10.1. Modelo de entrevista usada en la UCN

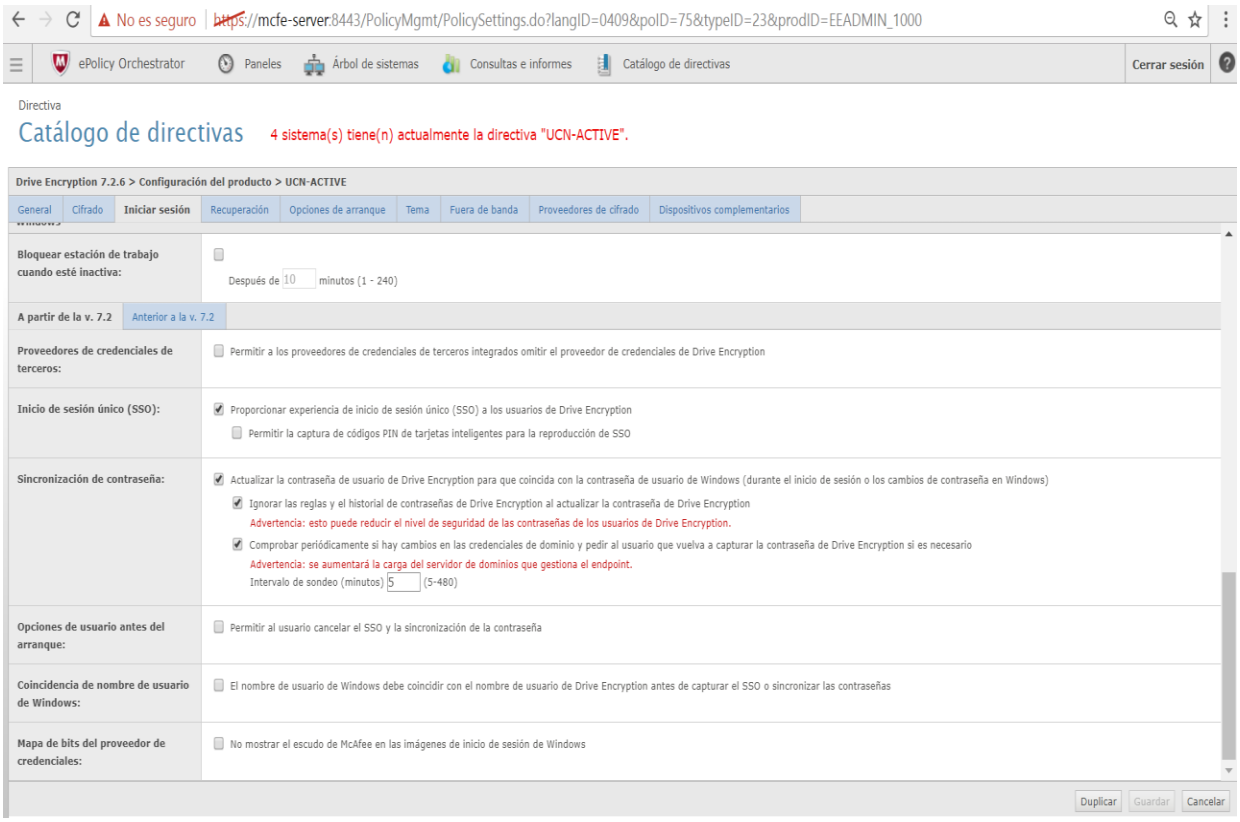
N°	Pregunta
1	¿Cuántas computadoras portátiles tiene de su propiedad la universidad?
2	¿Estas computadoras portátiles a que personal están asignadas?
3	¿Este personal tiene permiso para llevarse la computadora portátil fuera de la UCN?
4	¿El personal que maneja información confidencial, además te tener asignado computadoras portátiles, tiene asignado computadoras de escritorio?
5	¿Qué sistemas operativos utilizan las computadoras portátiles y de escitorio en la UCN?
6	¿Se han extraviado computadoras portátiles dentro y fuera de la UCN?
7	¿Qué tan importante es la información que maneja la UCN?
8	¿Qué tanto les ha afectado el extravío de computadoras portátiles?
9	¿Qué controles de seguridad aplican en estas computadoras portátiles?
10	¿En su opinión que es cifrado de disco completo?
11	¿Aquí en la UCN cuentan con una aplicación de cifrado de disco completo?
12	¿En la infraestructura tecnológica actual, tiene espacio de crecimiento?
13	¿Su infraestructura es física o virtual?
14	¿Cuenta con licencia de Windows Server 2012 R2?

10.2. Manual Consola Epo McAfee.

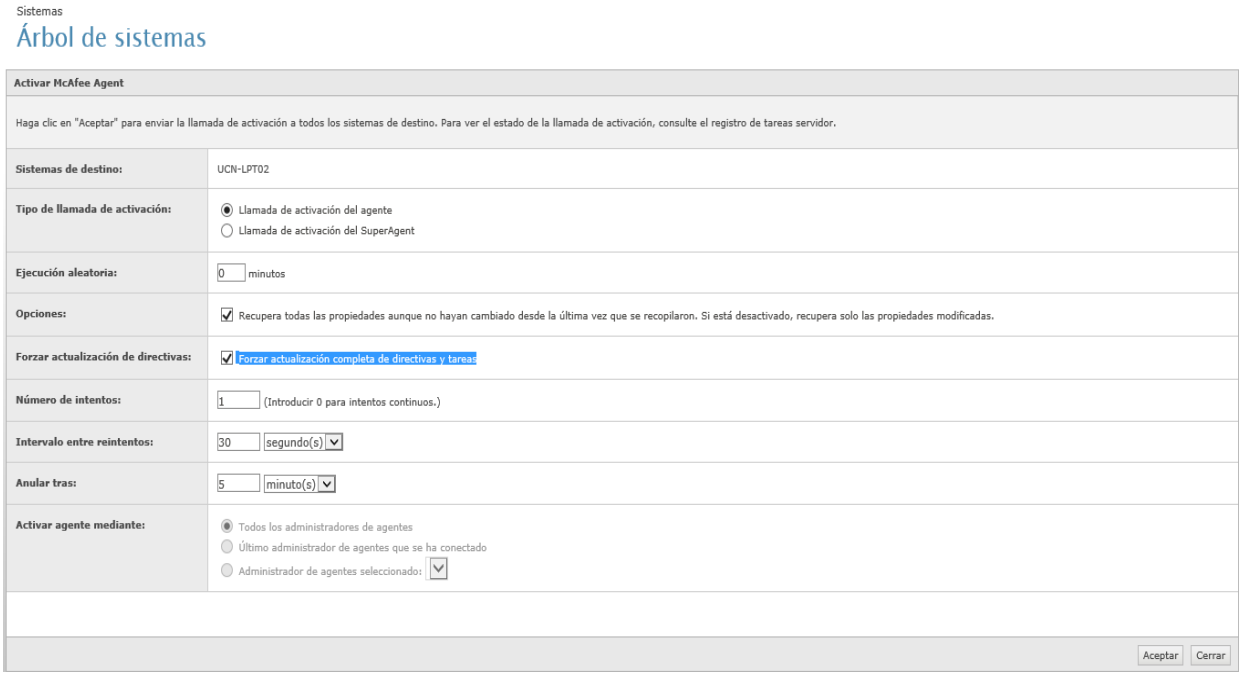
10.2.1. Cambio de clave de usuario de AD

En algunos casos que al realizar el cambio de clave en servidor de Active Directory y la clave no sea sincronizada con Drive Encryption, se deberán de realizar los siguientes pasos para la sincronización.

1. Realizar cambio de clave de usuario en Active Directory.
2. Verificar en la consola (**Catálogo de directivas→Drive Encryption 7.2.6→UCN-ACTIVE-->Iniciar sesión**).

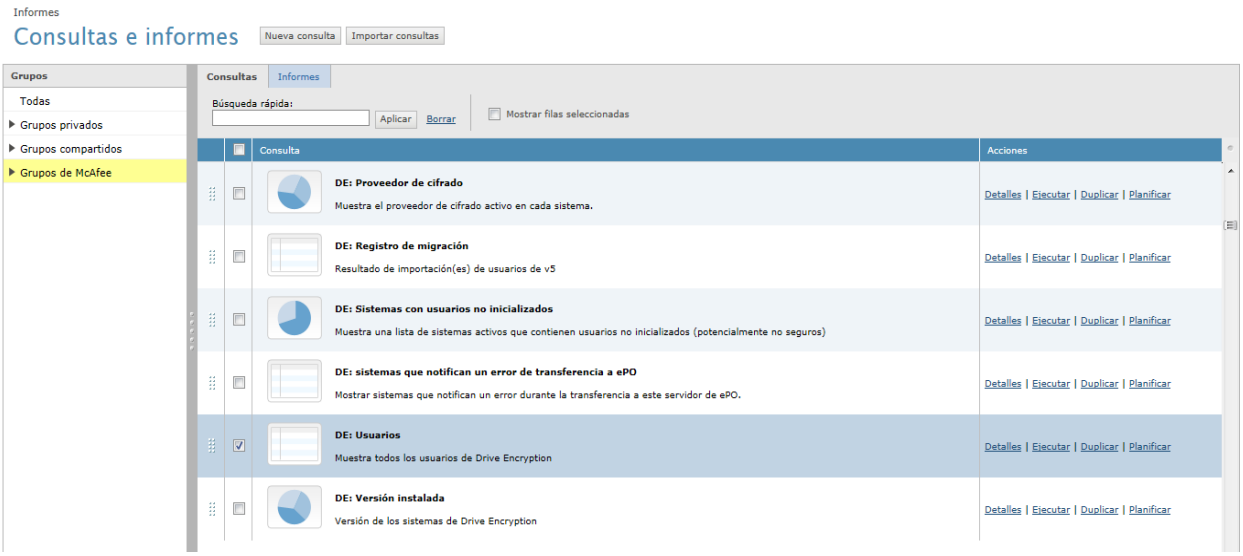


3. Actualizar las políticas como se muestra en la siguiente pantalla.

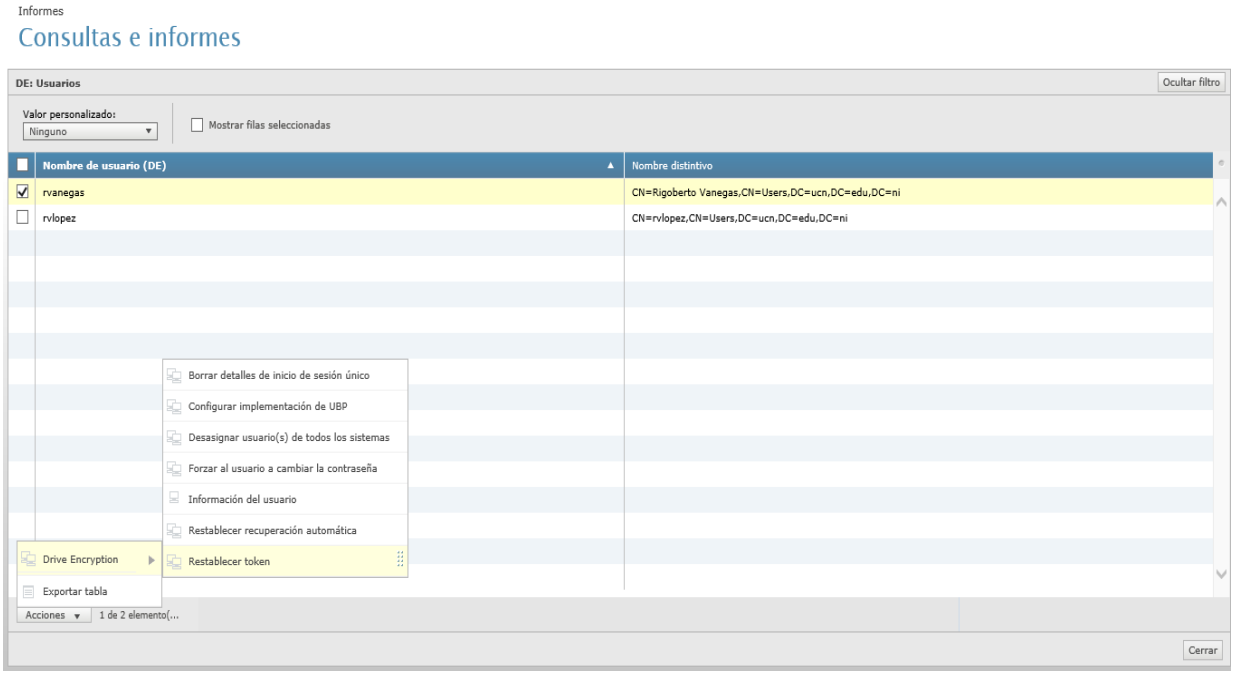


4. Se deberá de esperar 5 minutos para que la clave sea actualizada.
5. En caso que no se pueda ingresar con la clave del AD desde la pantalla de inicio de McAfee, se deberá de restablecer el token del usuario de la siguiente manera:

5.1. Conectarse a la consola Epo y dirigirse a la siguiente ruta: **Consultas e informes → Grupos de McAfee → Drive Encryption → DE:Usuarios → Ejecutar.**



5.2. Seleccionar el usuario que desea resetear la clave. **Acciones --> Drive Encryption --> Restablecer token.**



5.3. Una vez realizado el paso anterior, actualizar las políticas del equipo.

5.4. Reiniciar el equipo, al ingresar nuevamente deberá de ingresar con la clave por defecto y automáticamente le enviará a actualizar la clave. Esta clave de McAfee puede ser diferente de la clave del AD.

5.5. Actualizar nuevamente las políticas para que se realice la sincronización de la clave con la del AD.

5.6. Reiniciar el equipo, la clave que deberá utilizar será únicamente la clave del AD, esto porque se hace una sincronización de las claves y tiene prioridad el AD.

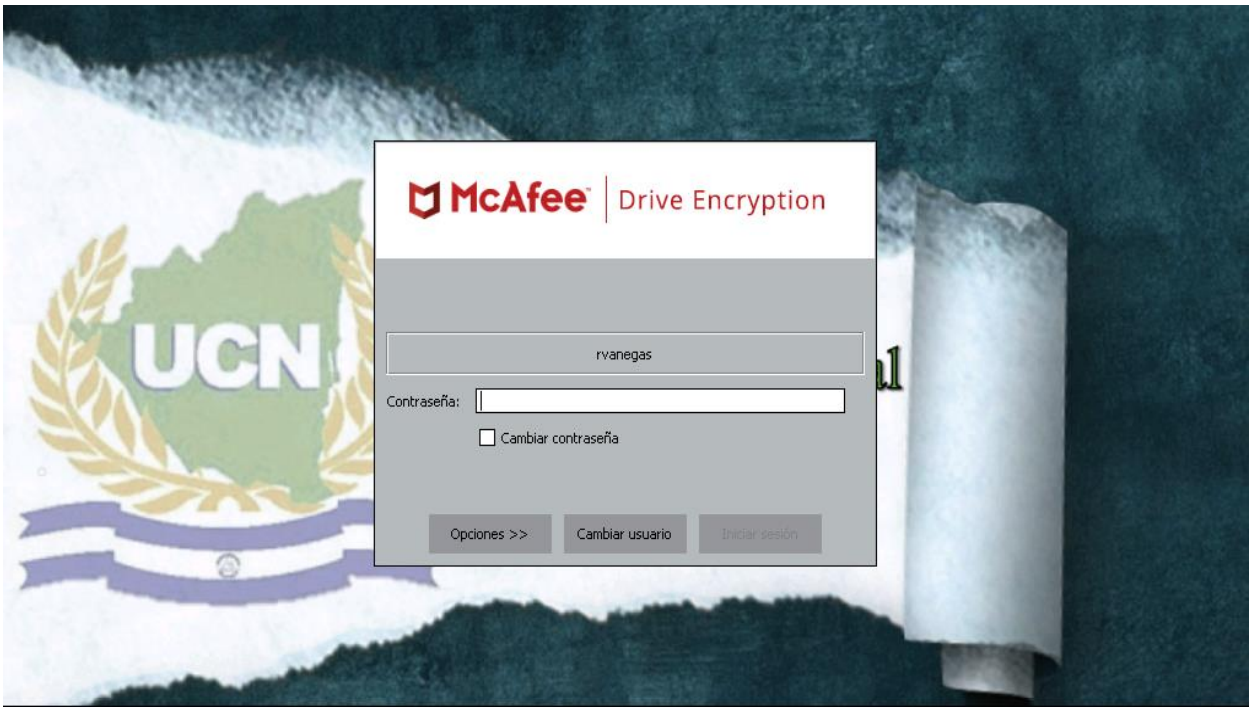
10.2.2. Recuperación de Drive Encryption

Este caso se aplica cuando no se pueda ingresar en la pantalla de inicio de McAfee Drive Encryption, ya sea por olvido de clave o que la clave no haya sido sincronizada. En este tipo de recuperación tenemos dos opciones para la recuperación e ingresar al equipo cifrado.

I. Equipo Cliente

En el equipo cliente se deberá de realizar los siguientes pasos:

1. Hacer click en el botón de **“Opciones”**, como se muestra en la siguiente pantalla:

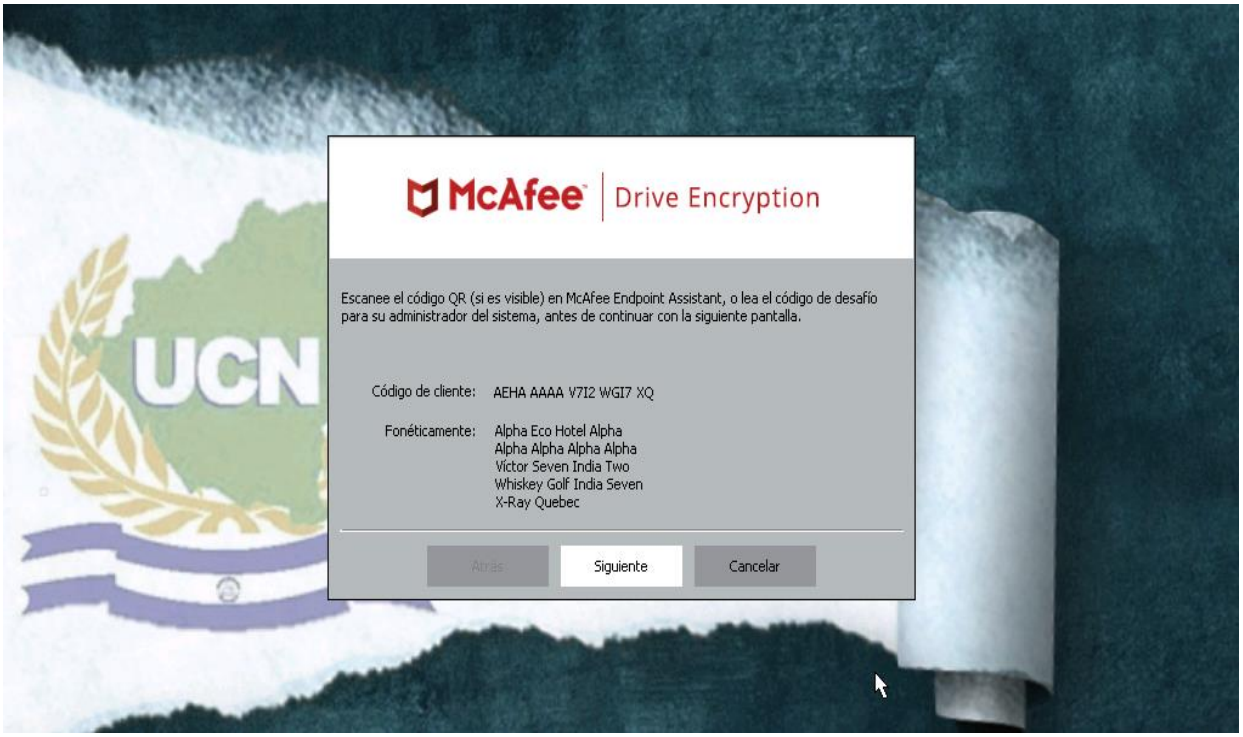


2. Hacer click en el botón de **“Recuperación”**

3. Nos aparecen dos opciones de recuperación, escogemos la primera opción y hacemos click en el botón **“Aceptar”.**

4. En la pantalla siguiente nos aparece un **"Código de Cliente"**, este código es el que vamos a utilizar para ingresarlo en el servidor de consola Epo. Continuamos con el paso **"II Servidor Consola Epo"**.

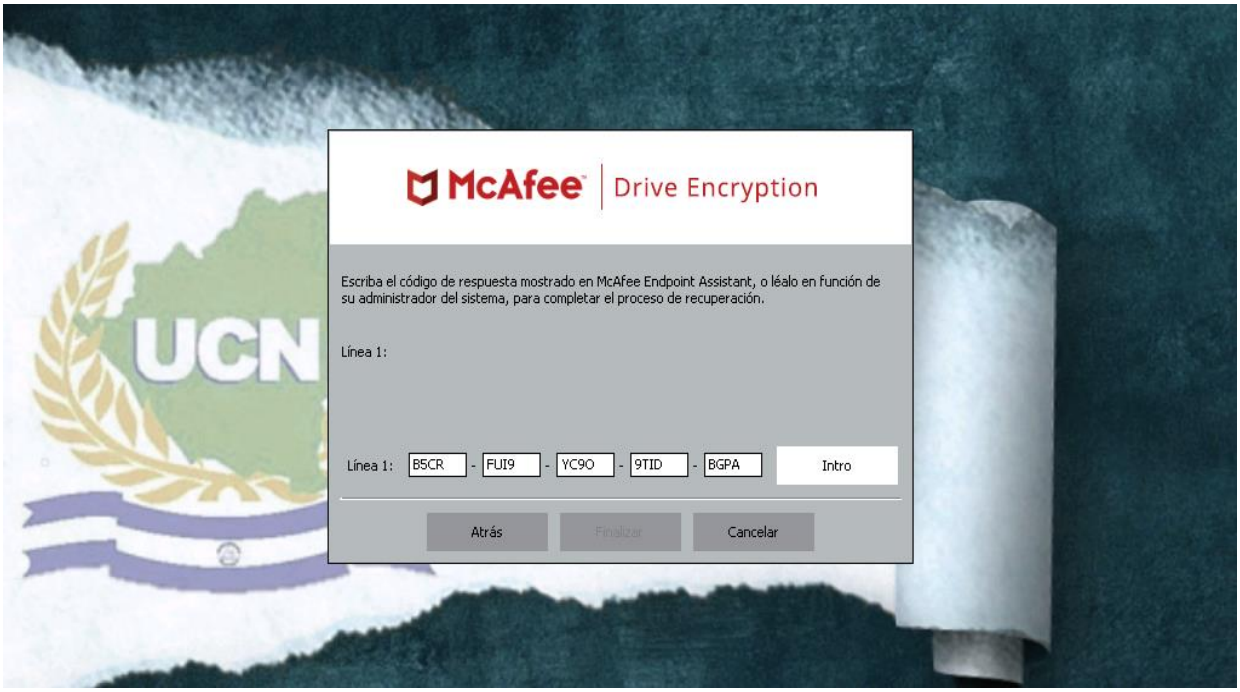
   El código es el siguiente: **AEHAAAAAV7I2WGI7XQ**



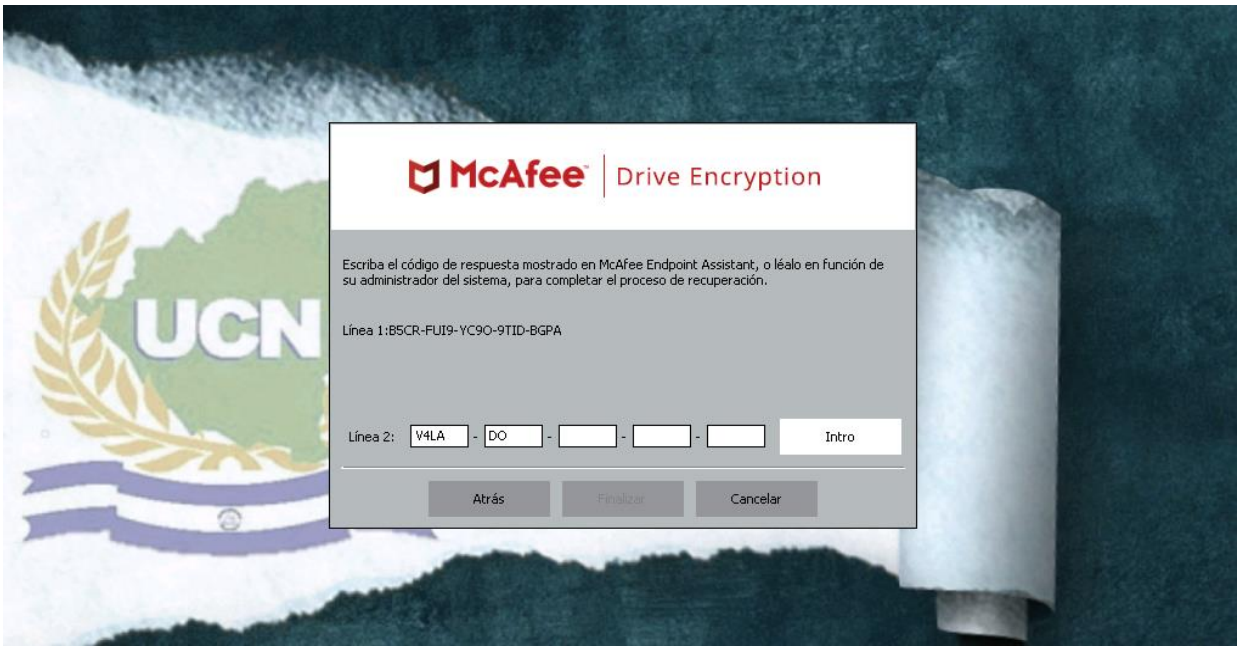
5. En la pantalla anterior, hacemos click en **"Siguiente"** y digitamos el código de respuesta proporcionado en el **paso 5** de **"II Servidor Consola Epo"**.

   Código de respuesta:

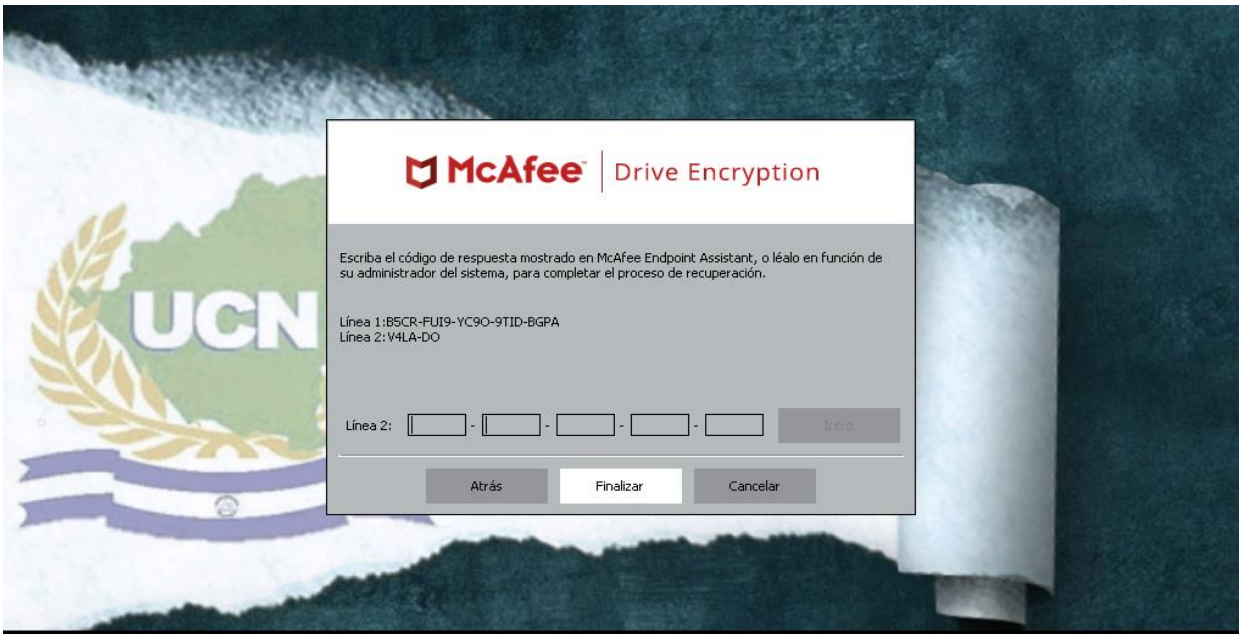
   Línea 1: B5CR-FUI9-YC9O-9TID-BGPA
   Línea 2: V4LA-DO

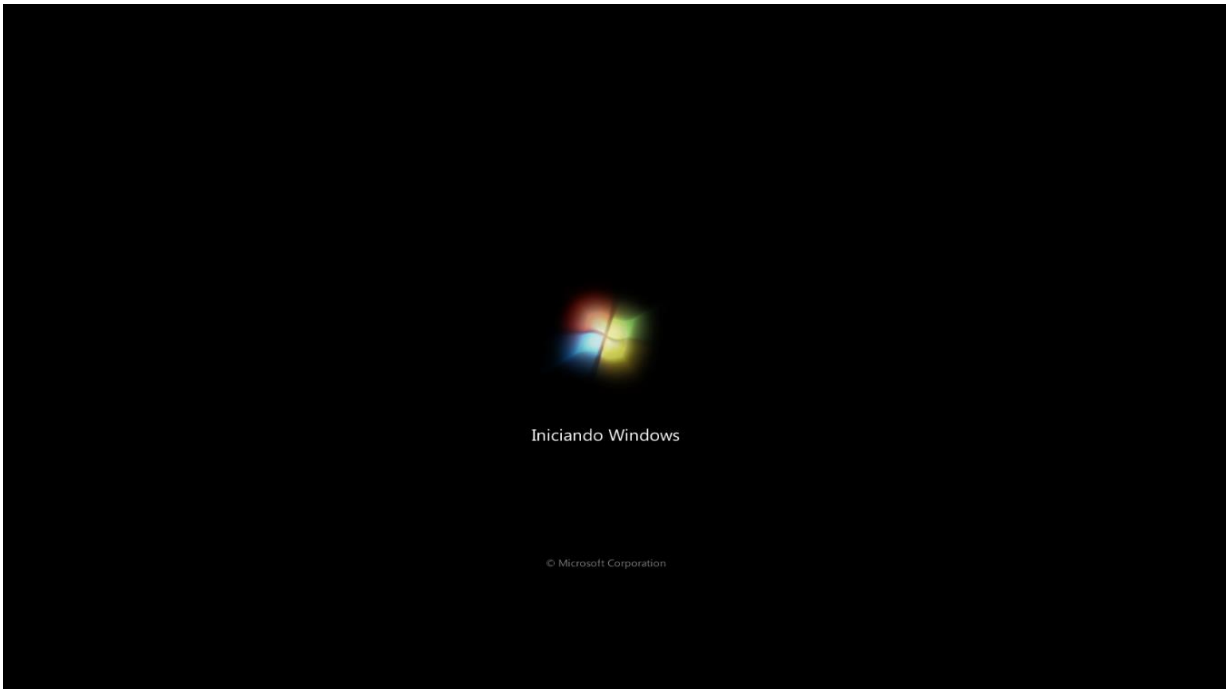


6. Una vez que digitó la Línea 1, hacer click en **“Intro”**, si el código se digitó correctamente pasará a la pantalla siguiente donde se digitará la Línea 2. Hacer click en **“Intro”**.



7. Si los códigos se digitaron correctamente, pasará a la siguiente pantalla. Una vez en esta pantalla, hacer click en **“Finalizar”** para ingresar al equipo. Una vez dentro del equipo se deberán de actualizar las políticas para que las claves sean sincronizadas.

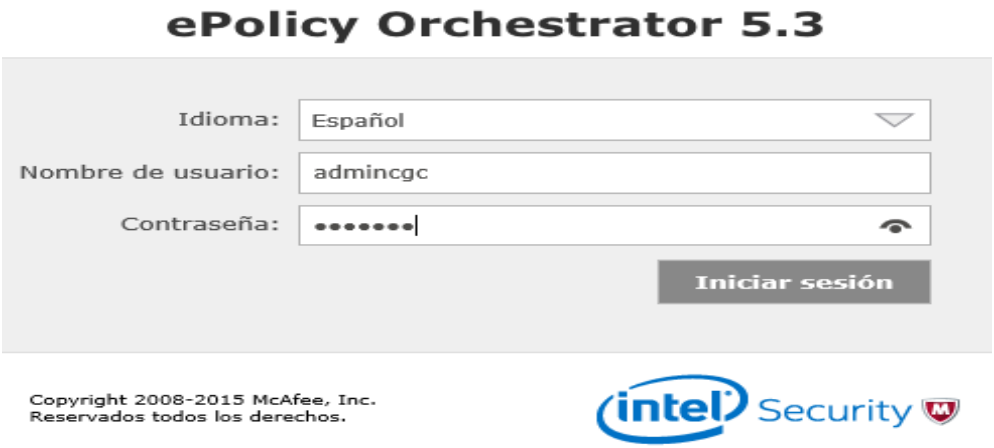




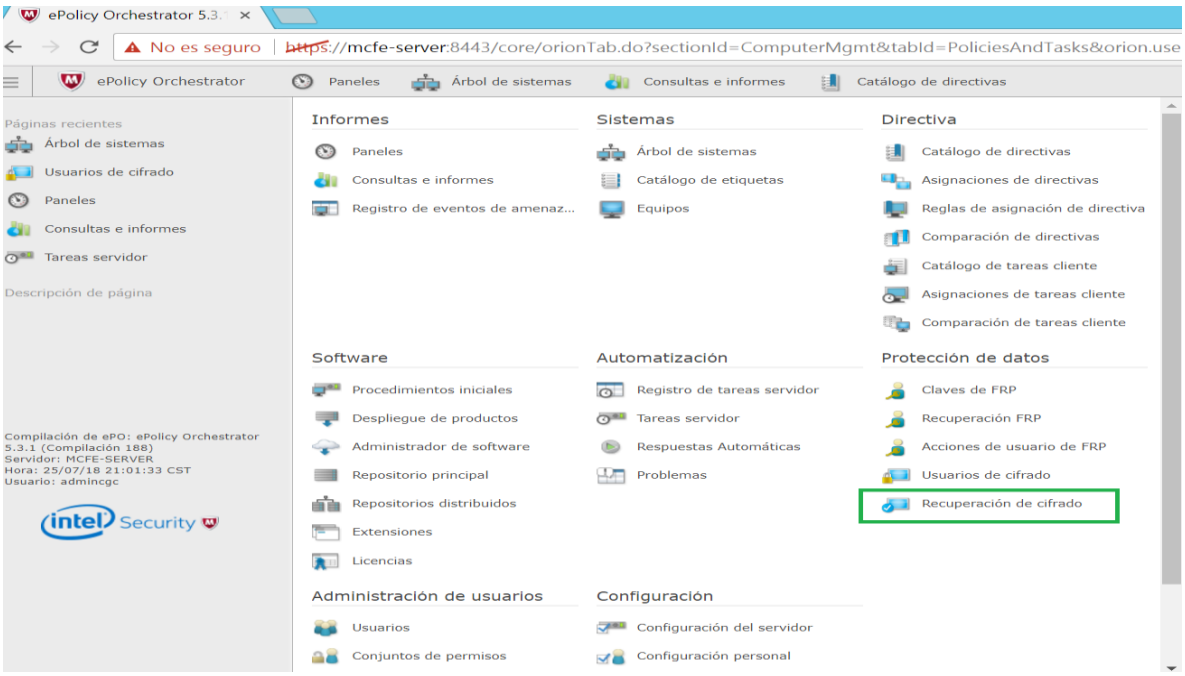
II. Servidor Consola Epo

Con el código de cliente que nos proporcionan en **“I Equipo Cliente”**, continuamos con los siguientes pasos:

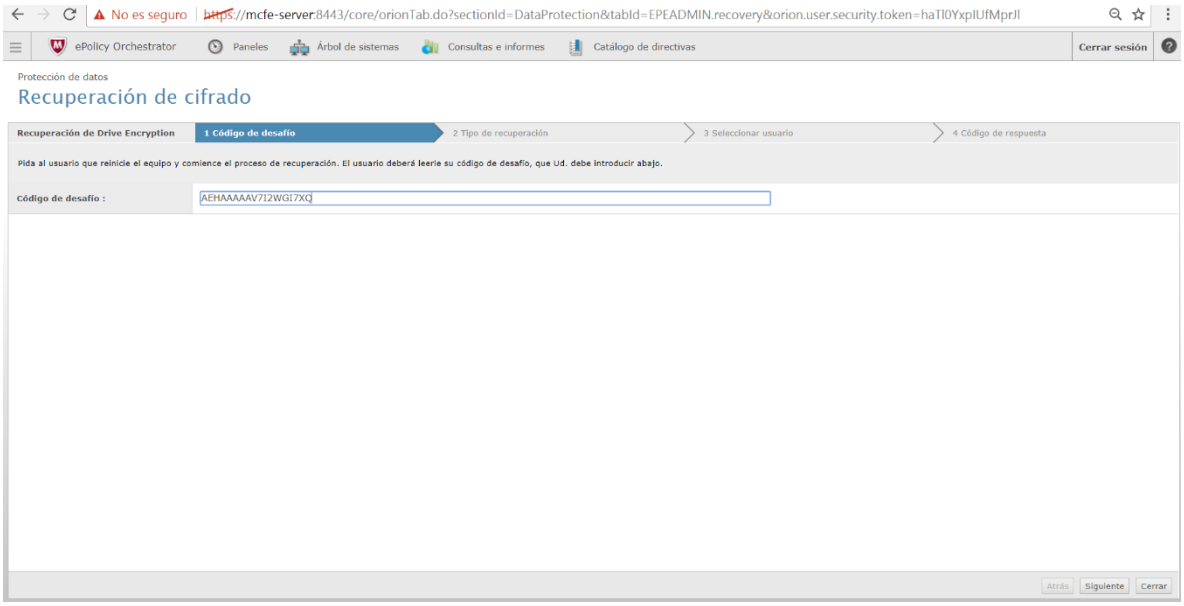
1. Ingresar a la consola Epo con usuario con permisos administrativos.



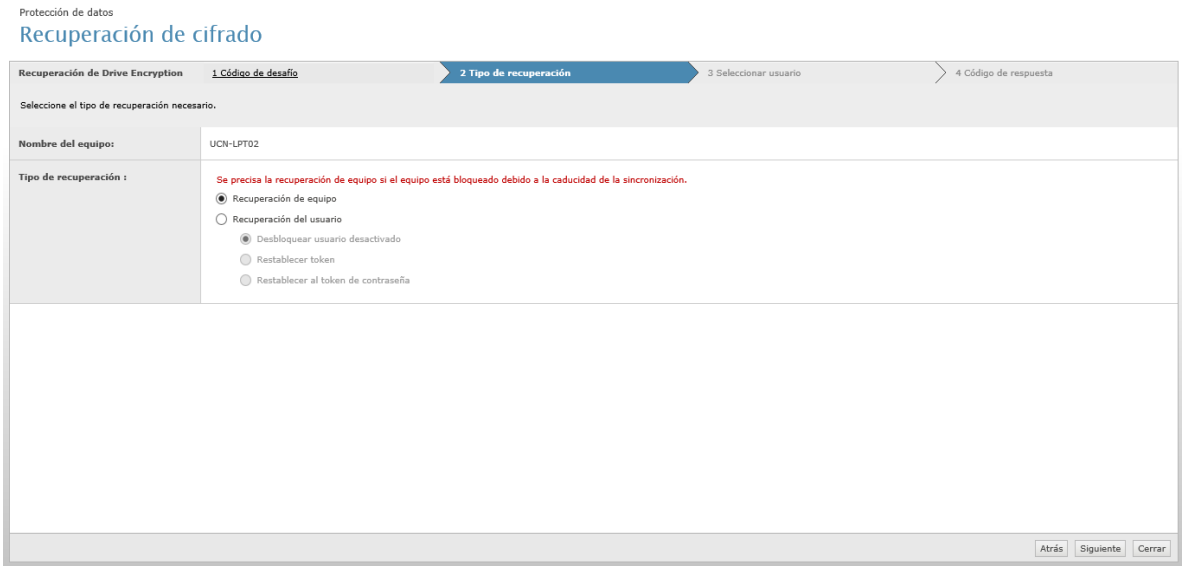
2. Ingresar a la siguiente ruta: Menu → **Protección de datos** → **Recuperación de cifrado.**



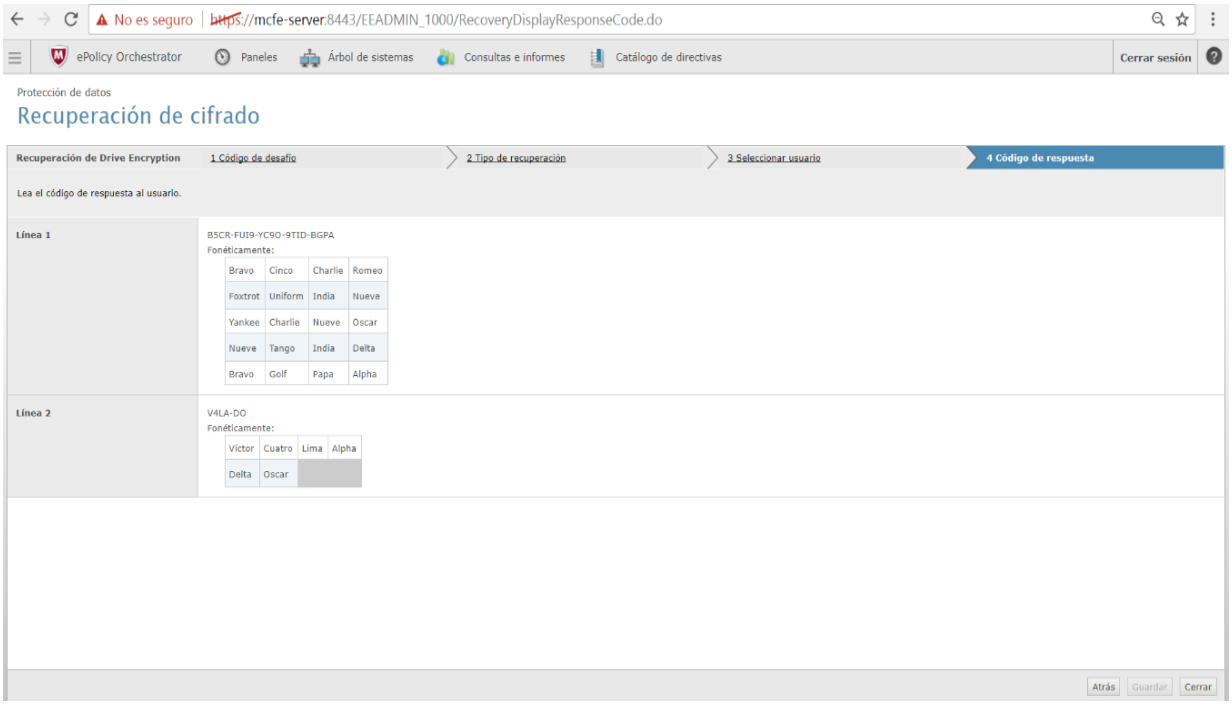
3. En esta pantalla se deberá de escribir el código de desafío proporcionado por el equipo que se desea recuperar, si el código es válido se pasará a la siguiente pantalla.



4. En este paso se deberá de seleccionar el tipo de recuperación. En este caso seleccionamos la primera opción, **“Recuperación de equipo”** y hacemos click en el botón de **“Siguiente”**.



5. En la siguiente pantalla nos regresa un **“Código de respuesta”**, este código es el que debemos ingresar en el equipo cliente para poder ingresar al equipo. Nos regresamos al **paso 5** de **“I Equipo Cliente”**.



6. El código de respuesta proporcionado por la consola se deberá de digitar en el equipo cliente. Si los pasos se realizaron correctamente, se ingresará sin ningún problema al equipo cliente. Cabe señalar que este método únicamente funciona una sola vez para ingresar al equipo.

10.2.3. Procedimiento de Recuperación en los siguientes escenarios:

10.2.3.1. En caso de daño completo del equipo cifrado con disco en buen estado no es necesario aplicar el procedimiento de descifrado de disco duro.

Para la recuperación de los datos en este caso se debe realizar el siguiente procedimiento:

1. Extraer el disco duro del equipo laptop dañada y colocarlo en un equipo con características similares.
2. Encender el equipo con el disco duro cifrado, le pedirá credenciales de McAfee Drive Encryption.

3. Ingresar con el usuario administrador local para iniciar el sistema. En caso que no pueda ingresar tiene la opción recuperación de equipo o usuario para ingresar. Únicamente se podrá ingresar con usuarios autorizados y que se tenga acceso a la consola ePO.

4. Una vez dentro del sistema operativo podrá realizar el respaldo de la información contenida en el disco duro.

   Nota: También se puede hacer el respaldo utilizando el procedimiento de descifrado de disco duro, llegando al paso 9 pero en vez de **"Remove DE"**, se accede al disco con la información y se puede hacer el respaldo.

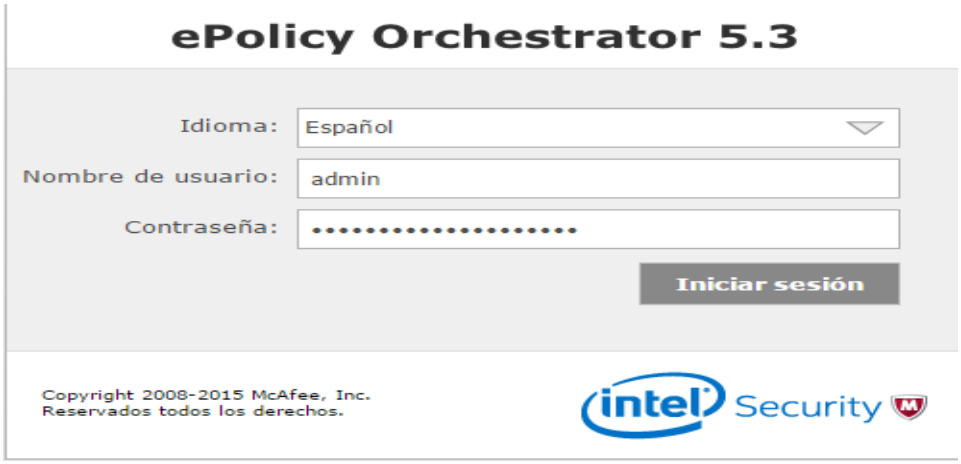
10.2.3.2. En caso de sistema operativo corrupto se debe aplicar el procedimiento de descifrado de disco duro.

10.2.3.3. En caso de daño completo del equipo cifrado con disco en buen estado se debe aplicar el procedimiento de descifrado de disco duro.

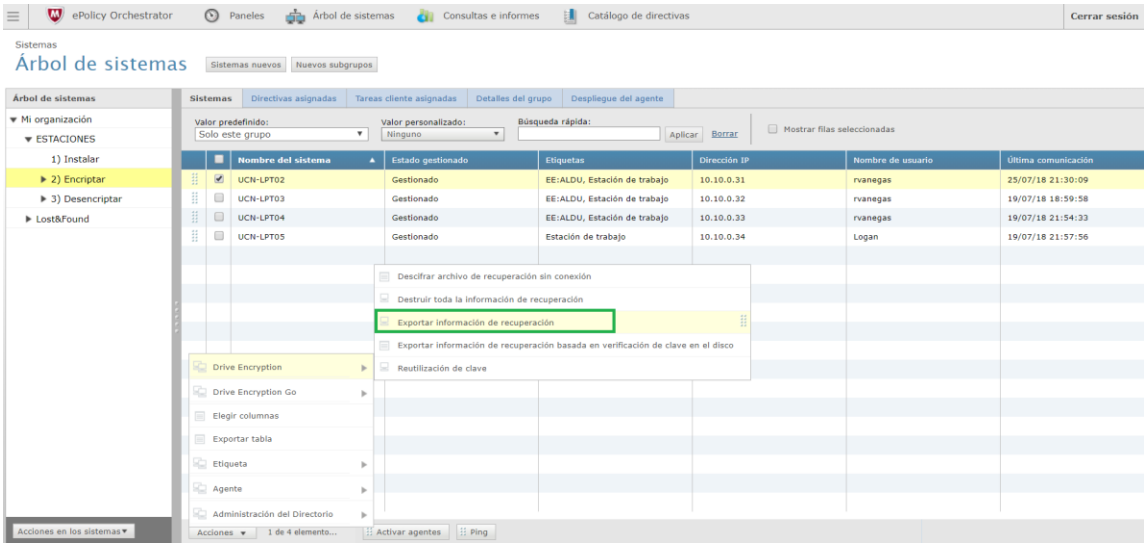
Este procedimiento aplica para el caso 10.2.3.2 y 10.2.3.3. La única diferencia es que en el caso 10.2.3.3 se tendría que extraer el disco duro cifrado y colocarlo en un equipo laptop con características similares, mientras que en el caso 10.2.3.2 se trabaja en el mismo equipo.

10.2.4. Procedimiento de Descifrado de Disco Duro.

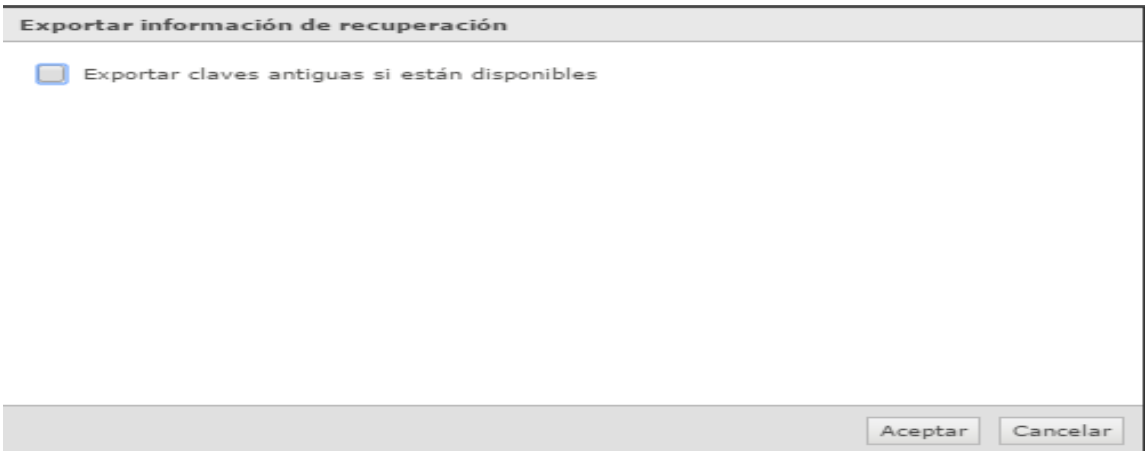
1. Conectarse a la consola Epo con un usuario con permisos administrativos.

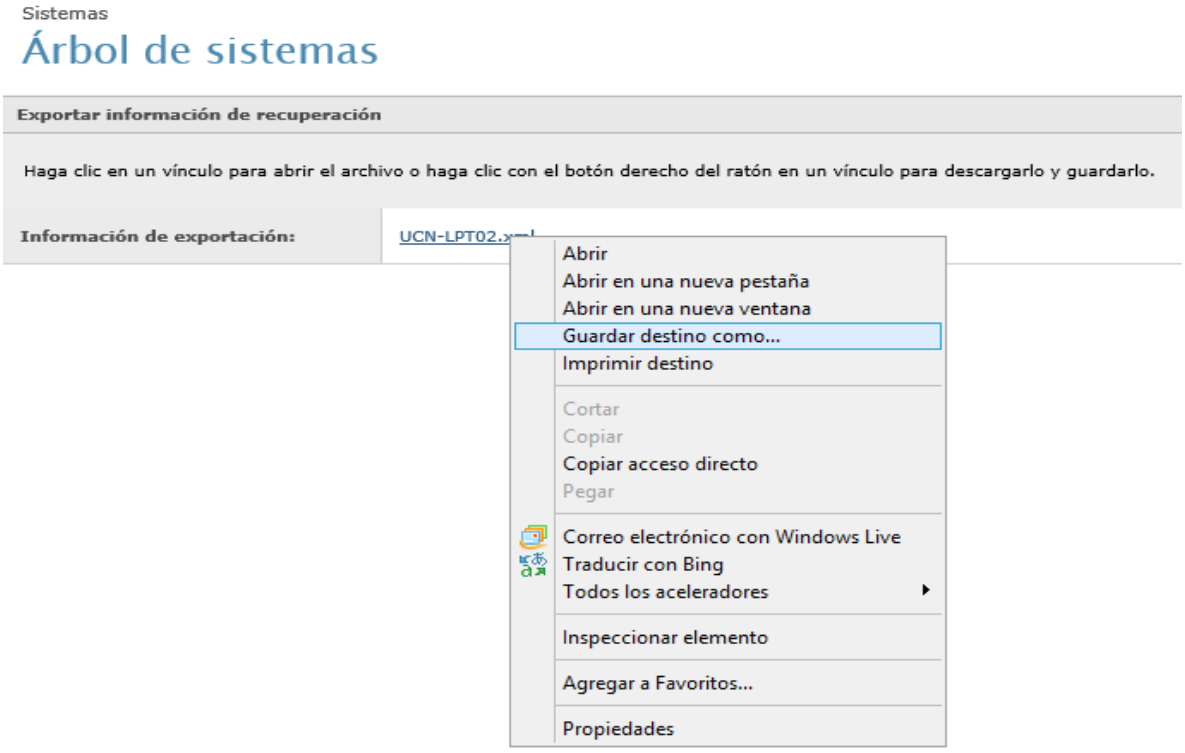


2. Ir a la opción “Árbol de sistemas” ---> Estaciones ---> Encriptar y seleccionar la computadora que se le aplicará el procedimiento. Seleccionar: “Acciones” --->Drive Encryption ---> Exportar información de recuperación.



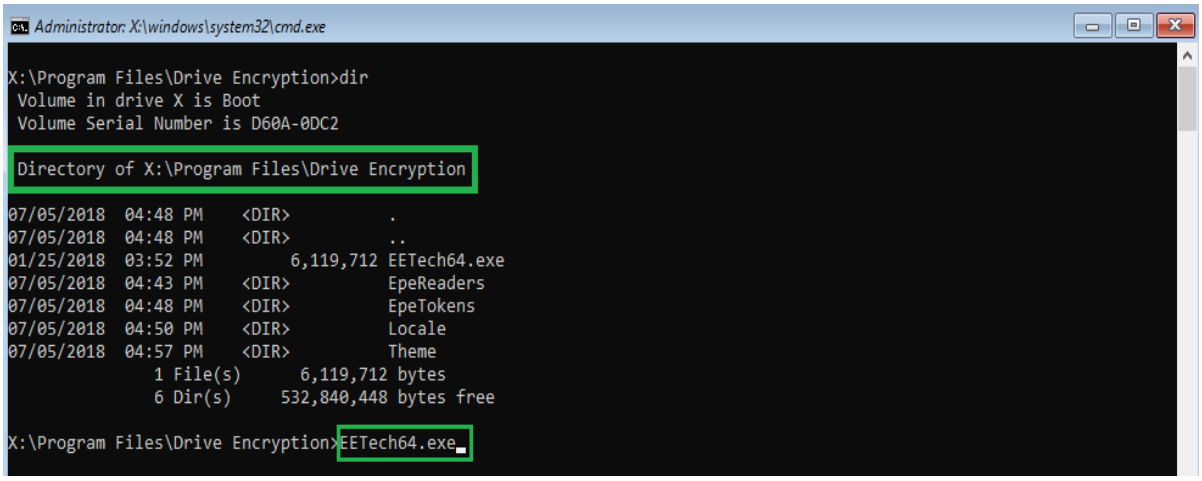
3. Una vez realizado el paso anterior, se deberá de guardar el archivo .xml en una memoria USB o cualquier otro medio.



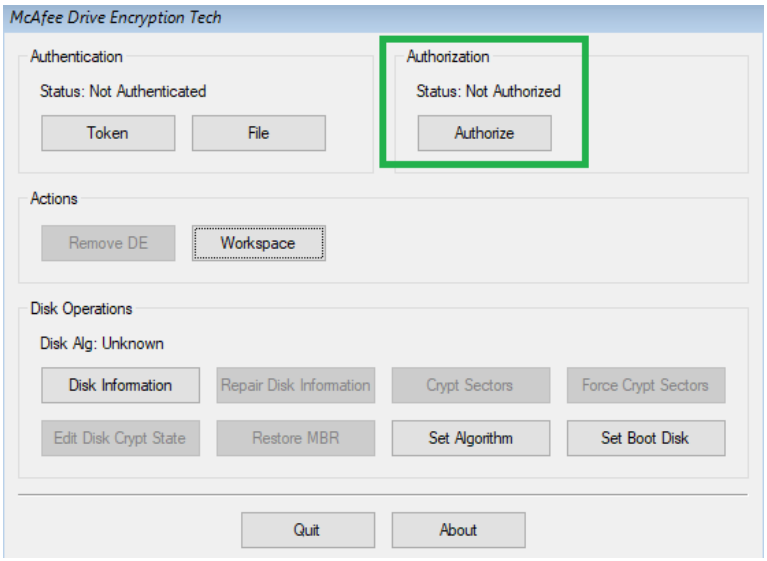


4. Arrancar el dispositivo UCN-LPT02 con la imagen EETech, una vez que inicie, ingresar a la siguiente desde la línea de comando al siguiente directorio: \Program Files\Drive Encryption>

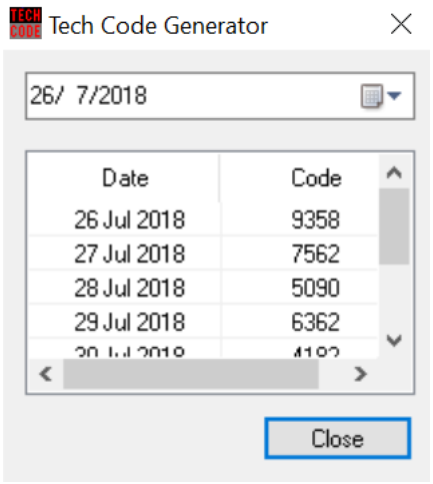
Una vez en ese directorio, ejecutar EETech64.exe



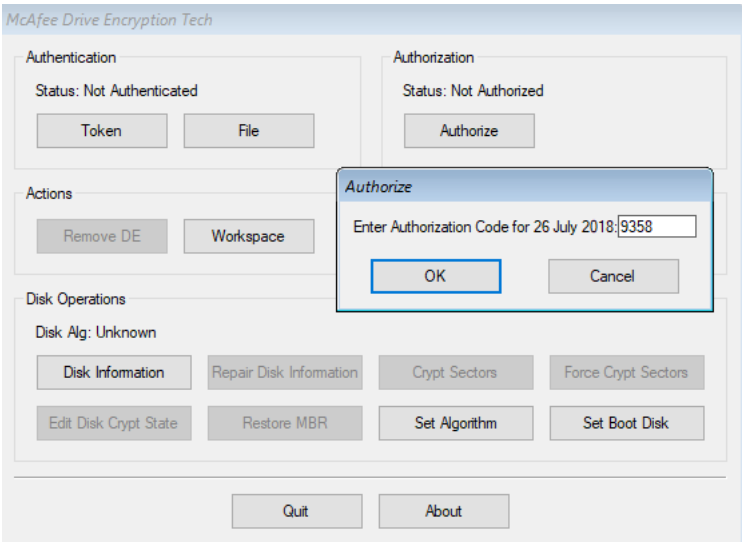
5. Una vez ejecutado el comando anterior, se va a desplegar la siguiente pantalla. Es necesario realizar la autorización para utilizar las opciones que se encuentran desactivadas, como por ejemplo “Remove DE”.



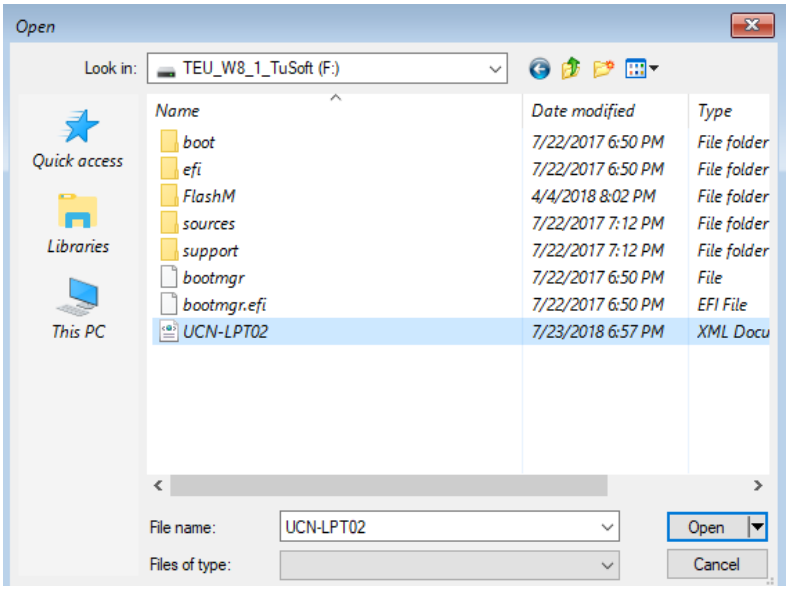
6. Para realizar la autorización es necesario el archivo .xml del dispositivo que se guarda en el paso #3 de este procedimiento y correr la aplicación “EETechCode”, esta aplicación nos muestra el código del día que debemos usar.



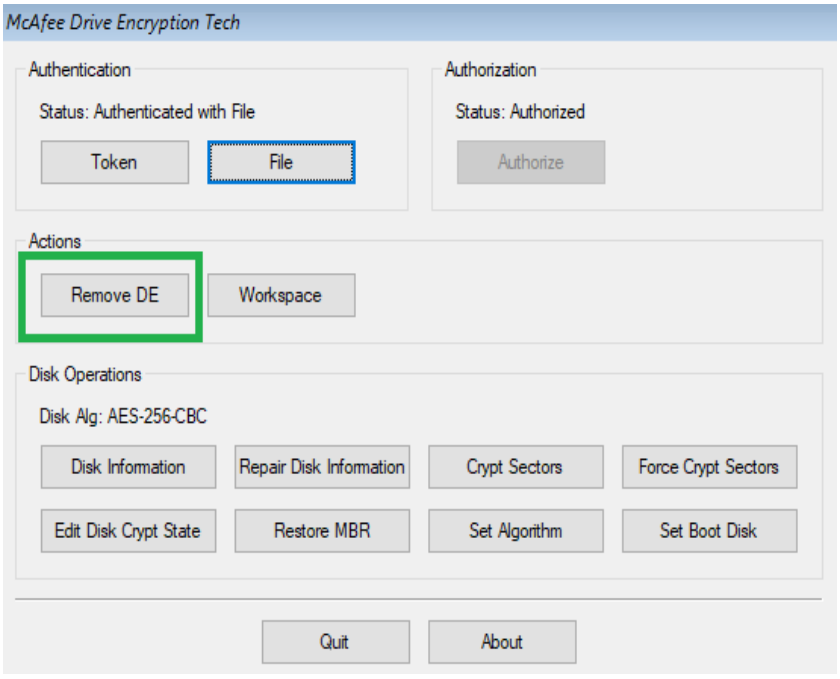
7. Click en “Authorization”, “Authorize”, escribir el código del paso #6, click en Ok.



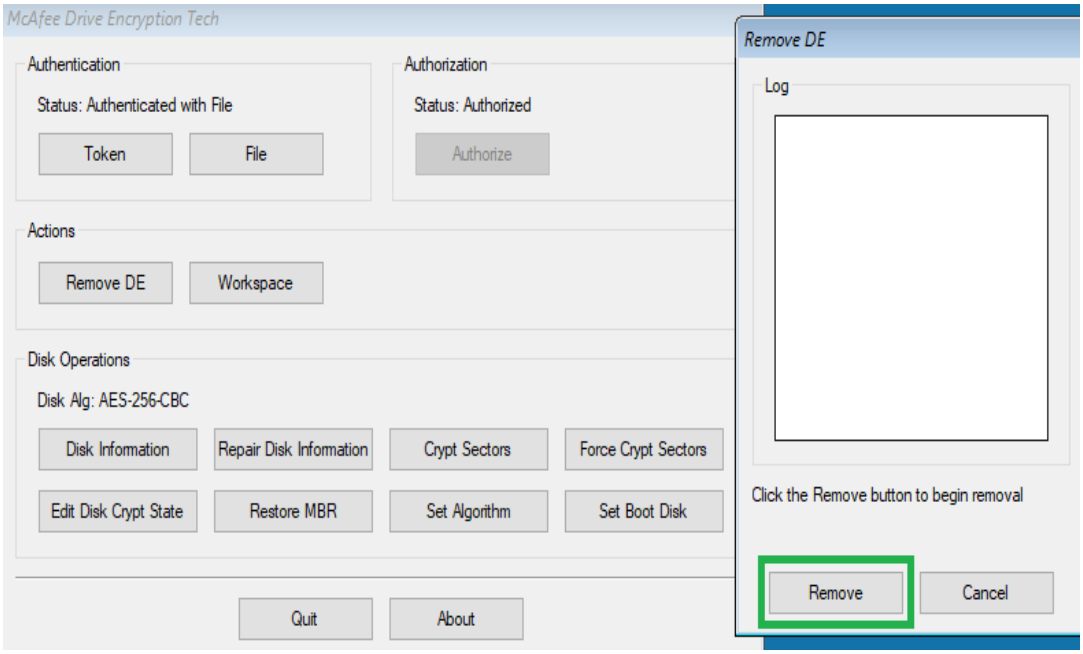
8. Opción “Authentication”, “File”, seleccionar el xml guardado en el paso #3 y abrirlo.

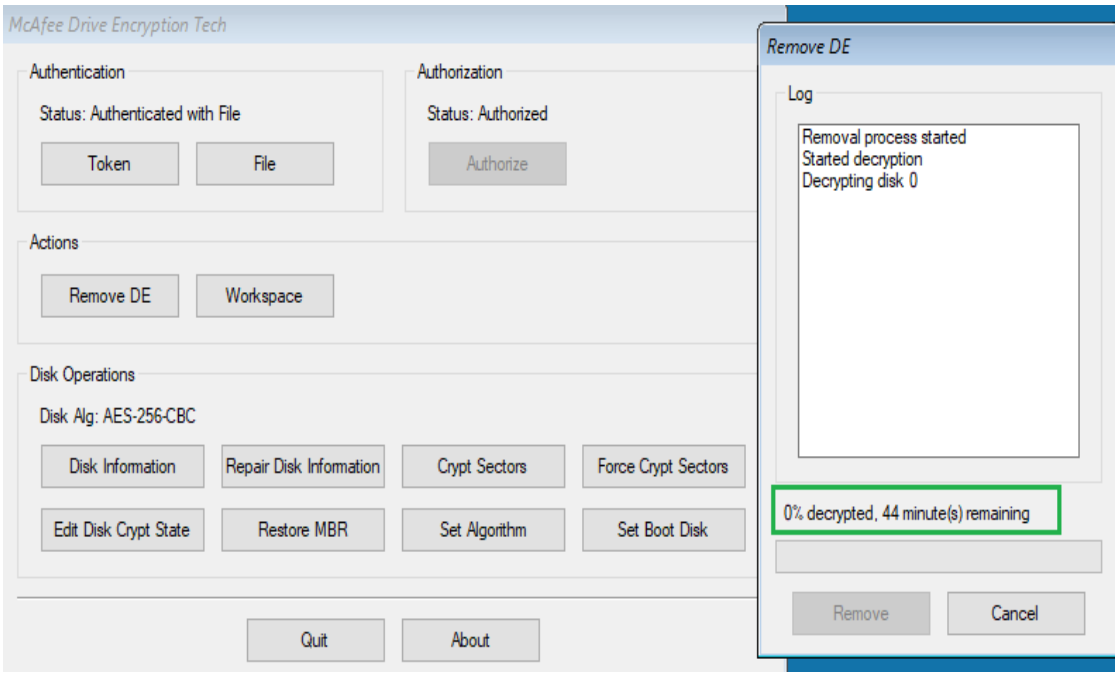


9. Una vez realizado el paso anterior, se activan todas las opciones, incluida la opción “Remove DE”, la seleccionamos para remover el cifrado del disco duro.

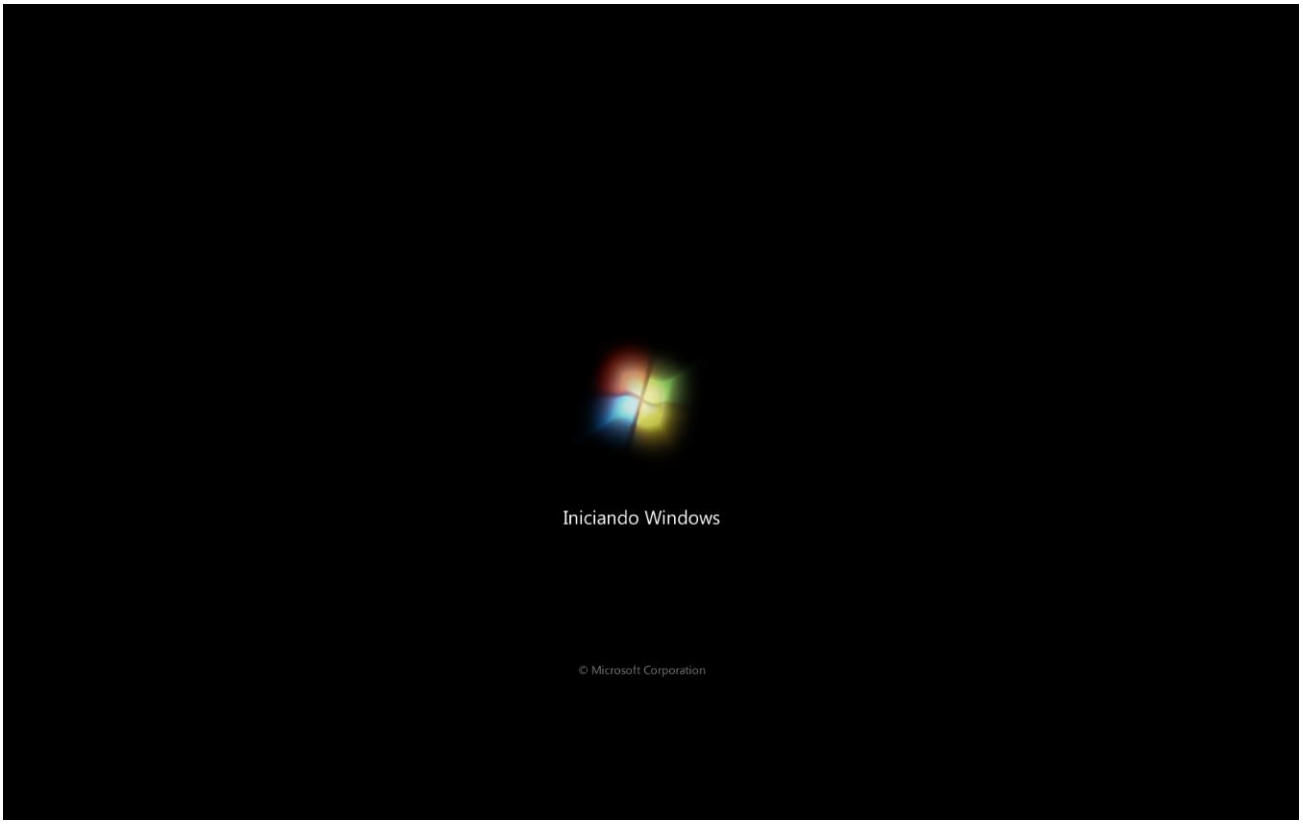


10. Iniciará el proceso, este tardará aproximadamente el mismo tiempo que duró la encriptación. Esto dependerá de la capacidad del disco y de los recursos del dispositivo. En este caso se estima que terminará en 44 minutos.

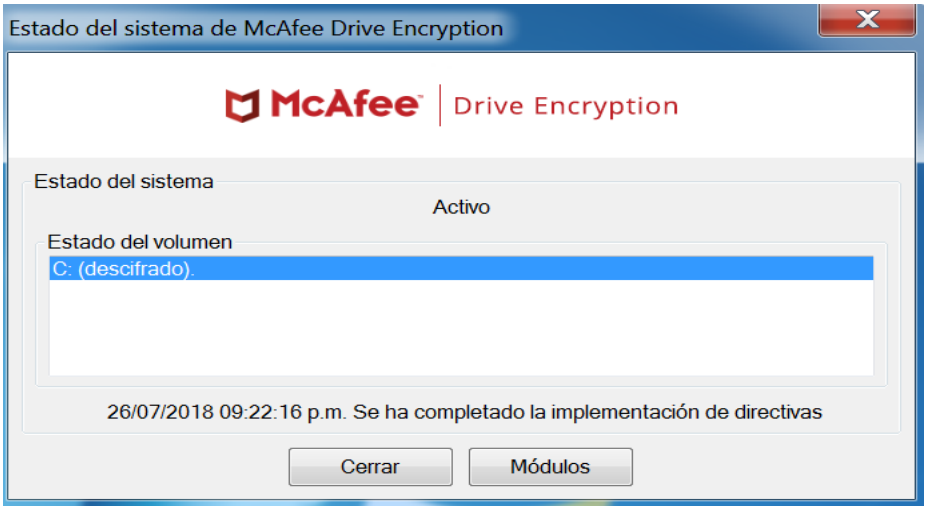




11. Una vez finalizado el paso anterior de manera satisfactoria, únicamente hay que reiniciar el dispositivo portátil, si el sistema operativo esta funcional, ingresará directamente al sistema operativo. En las siguientes pantallas se puede observar que carga directamente el sistema operativo y el disco se encuentra descifrado.



12. Una vez finalizado el paso anterior de manera satisfactoria, únicamente hay que reiniciar el dispositivo portátil, si el sistema operativo esta funcional, ingresará directamente al sistema.



Sistemas

Árbol de sistemas

Drive Encryption > UCN-LPT02

Propiedades | **Discos**

Disco de Drive Encryption : Disco de Drive Encryption: Descripción

Número de modelo	Número de serie	Tamaño (MB)	Estado (disco)
VMware Virtual S		30.720	Descifrado

Resumen Personalizar

UCN-LPT02
Resumen de conformidad de McAfee Agent

Dirección IP:	10.10.0.31
Nombre de dominio:	UCN
Ubicación del sistema:	Mi organización\ESTACIONES\1) Instalar

Propiedades del sistema | **Productos** | Eventos de amenazas | McAfee Agent | Driv

Producto	Versión
Agent	5.5.0.447
Drive Encryption: Windows	7.2.4.2
Drive Encryption Agent	7.2.4.2
Drive Encryption Go	7.2.4.2

Propiedades de los productos para Agent